



TR-4931: VMware Cloud on Amazon Web Services とゲストコネクトによる災害復旧

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目次

TR-4931: VMware Cloud on Amazon Web Services とゲストコネクトによる災害復旧	1
概要	1
前提、前提条件、コンポーネントの概要	1
SnapCenterでDRを実行する	1
SnapMirror関係と保持スケジュールを構成する	2
オンプレミスで Windows SnapCenterサーバーを展開および構成します。	10
Veeam バックアップ サーバーの導入と構成	19
BlueXP backup and recoveryツールと構成	30
災害復旧のためのSnapCenterデータベースバックアップ	31
フェイルオーバー	39
Veeam の完全復元でアプリケーション VM を復元する	42
SQL Server アプリケーション データを復元する	55
Oracleアプリケーションデータの復元	64
フェイルバック	70
まとめ	70

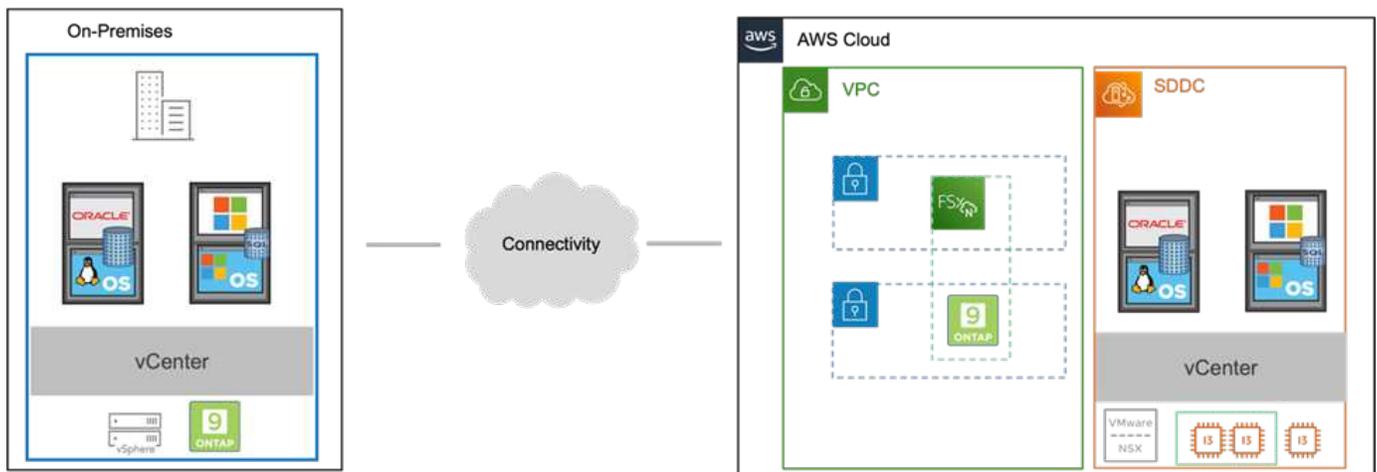
TR-4931: VMware Cloud on Amazon Web Services とゲストコネクタによる災害復旧

大規模な障害が発生した場合にビジネスクリティカルなアプリケーションを迅速に復旧できるようにするために、組織にとって実証済みの災害復旧 (DR) 環境と計画が不可欠です。このソリューションは、オンプレミスと VMware Cloud on AWS の両方で、VMware および NetApp テクノロジーに重点を置いた DR ユースケースのデモンストレーションに重点を置いています。

概要

NetApp は VMware との統合において長い歴史を誇ります。これは、仮想化環境のストレージ パートナーとして NetApp を選択した何万もの顧客によって証明されています。この統合は、クラウド内のゲスト接続オプションや、最近の NFS データストアとの統合でも継続されます。このソリューションは、一般的にゲスト接続ストレージと呼ばれるユースケースに重点を置いています。

ゲスト接続ストレージでは、ゲスト VMDK は VMware によってプロビジョニングされたデータストアに展開され、アプリケーション データは iSCSI または NFS に格納され、VM に直接マップされます。次の図に示すように、Oracle および MS SQL アプリケーションを使用して DR シナリオを説明します。



前提、前提条件、コンポーネントの概要

このソリューションを展開する前に、コンポーネントの概要、ソリューションを展開するために必要な前提条件、およびこのソリューションを文書化する際に行われた仮定を確認してください。

["DRソリューションの要件、前提条件、および計画"](#)

SnapCenterでDRを実行する

このソリューションでは、SnapCenter は SQL Server および Oracle アプリケーション データに対してアプリケーション 整合性のあるスナップショットを提供します。この構成は、SnapMirror テクノロジーと組み合わせることで、オンプレミスの AFF と FSx ONTAP クラスタ間の高速データ レプリケーションを実現します。さらに、Veeam Backup & Replication は仮想マシンのバックアップと復元機能を提供します。

このセクションでは、バックアップとリストアの両方におけるSnapCenter、 SnapMirror、および Veeam の構成について説明します。

次のセクションでは、セカンダリ サイトでフェイルオーバーを完了するために必要な構成と手順について説明します。

SnapMirror関係と保持スケジュールを構成する

SnapCenter は、長期アーカイブと保持を目的として、プライマリ ストレージ システム内 (プライマリ > ミラー) およびセカンダリ ストレージ システム (プライマリ > ボールト) のSnapMirror関係を更新できます。そのためには、 SnapMirrorを使用して、宛先ボリュームとソース ボリューム間のデータ複製関係を確立し、初期化する必要があります。

ソースと宛先のONTAPシステムは、Amazon VPC ピアリング、トランジットゲートウェイ、AWS Direct Connect、または AWS VPN を使用してピアリングされたネットワーク内にある必要があります。

オンプレミスのONTAPシステムと FSx ONTAPの間にSnapMirror関係を設定するには、次の手順が必要です。

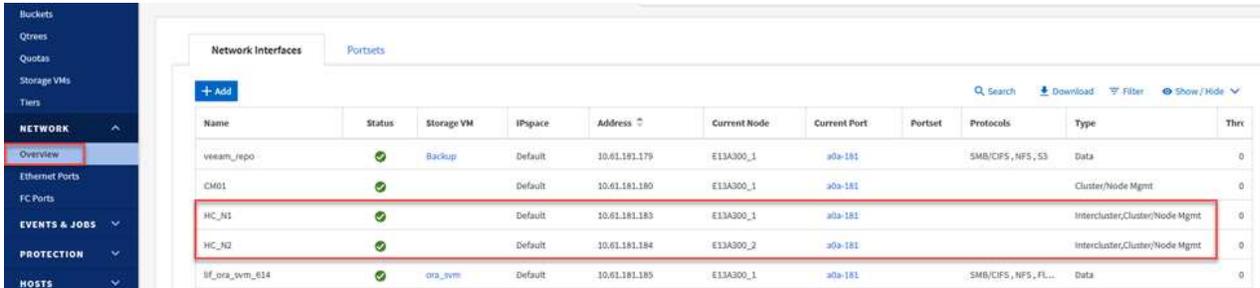


参照 ["FSx ONTAP – ONTAPユーザーガイド"](#)FSx とのSnapMirror関係の作成の詳細については、こちらをご覧ください。

送信元と宛先のクラスタ間論理インターフェースを記録する

オンプレミスにあるソースONTAPシステムの場合、System Manager または CLI からクラスタ間 LIF 情報を取得できます。

1. ONTAP System Manager で、[ネットワークの概要] ページに移動し、FSx がインストールされている AWS VPC と通信するように設定されているタイプ: クラスタ間の IP アドレスを取得します。



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thru
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster/Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster/Cluster/Node Mgmt	0
lif_ora_vvm_614	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. FSx のクラスタ間 IP アドレスを取得するには、CLI にログインして次のコマンドを実行します。

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
      Logical      Status      Network      Current      Current      Is
Vserver  Interface  Admin/Oper  Address/Mask  Node          Port          Home
-----
FsxId0ae40e08acc0dea67
      inter_1    up/up      172.30.15.42/25  FsxId0ae40e08acc0dea67-01
                                     e0e          true
      inter_2    up/up      172.30.14.28/26  FsxId0ae40e08acc0dea67-02
                                     e0e          true
2 entries were displayed.
```

ONTAPとFSx間のクラスタピアリングを確立する

ONTAPクラスタ間のクラスタピアリングを確立するには、開始側のONTAPクラスタで入力した一意のパスフレーズを、他のピアクラスタで確認する必要があります。

1. 宛先FSxクラスタでピアリングを設定するには、`cluster peer create`指示。プロンプトが表示されたら、後でソースクラスタで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. ソースクラスタでは、ONTAP System Manager または CLI を使用してクラスタピア関係を確立できます。ONTAP System Manager から、[Protection] > [Overview] に移動し、[Peer Cluster] を選択します。

DASHBOARD

STORAGE

Overview

Volumes

LUNs

Consistency Groups

NVMe Namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

Overview

Intercluster Settings

Network Interfaces

IP ADDRESS

- 10.61.181.184
- 172.21.146.217
- 10.61.181.183
- 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- FsxId0ae40e08acc0dea67
- OTS02

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- 3

3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。
 - a. 宛先 FSx クラスターでピア クラスター関係を確認するために使用されたパスフレーズを入力します。

- b. 選択 `Yes`暗号化された関係を確認します。
- c. 宛先 FSx クラスターのクラスター間 LIF IP アドレスを入力します。
- d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。

- 4. 次のコマンドを使用して、FSx クラスターからクラスター ピア関係のステータスを確認します。

```
FSx-Dest::> cluster peer show
```

```
FSxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----
E13A300                1-80-000011 Available    ok
```

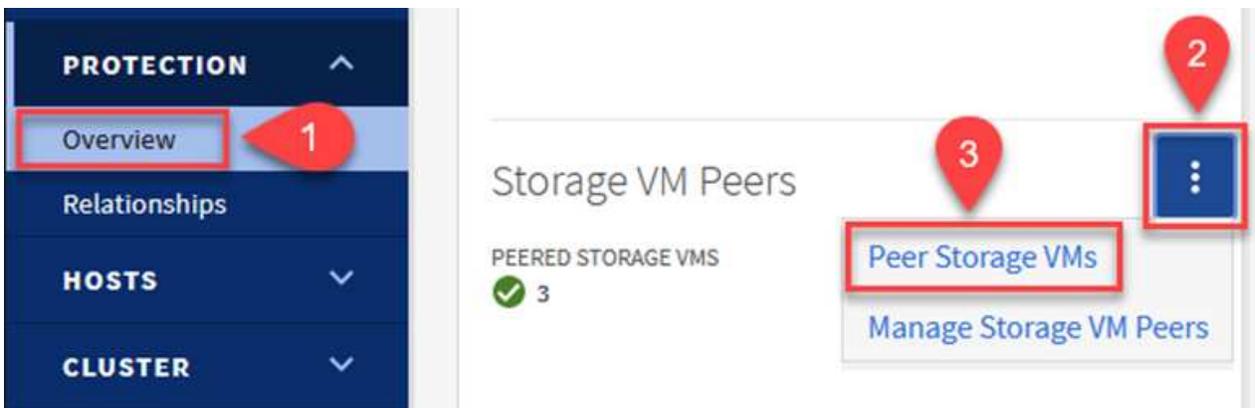
SVMピアリング関係を確立する

次の手順では、SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソース ストレージ仮想マシン間の SVM 関係を設定します。

1. ソース FSx クラスタから、CLI から次のコマンドを使用して SVM ピア関係を作成します。

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAPクラスタから、ONTAP System Manager または CLI のいずれかを使用してピアリング関係を受け入れます。
3. ONTAP System Manager から、[Protection] > [Overview] に移動し、[Storage VM Peers] の下の [Peer Storage VMs] を選択します。



4. ピア ストレージ VM のダイアログ ボックスで、必須フィールドに入力します。
 - ソースストレージVM
 - 宛先クラスター
 - 宛先ストレージVM

Peer Storage VMs



Local

Remote

CLUSTER
E13A300

STORAGE VM
Backup

CLUSTER
Fsxld0ae40e08acc0dea67 Refresh

STORAGE VM
svm_HCApPs

Peer Storage VMs

5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

スナップショット保持ポリシーを作成する

SnapCenter は、プライマリ ストレージ システム上にスナップショット コピーとして存在するバックアップの保持スケジュールを管理します。これは、SnapCenterでポリシーを作成するときに確立されます。SnapCenter は、セカンダリ ストレージ システムに保持されるバックアップの保持ポリシーを管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームとSnapMirror関係にある宛先ボリュームに関連付けられたSnapMirrorポリシーを通じて個別に管理されます。

SnapCenterポリシーを作成するときに、SnapCenterバックアップの作成時に生成される各スナップショットのSnapMirrorラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。



セカンダリ ストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先ボリュームに関連付けられたポリシー ルールと照合されます。

次の例は、SQL Server データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在するSnapMirrorラベルを示しています。

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Custom Label ⓘ

sql-daily

Error retry count 3 ⓘ

SQL Serverデータベース用のSnapCenterポリシーの作成の詳細については、"[SnapCenterのドキュメント](#)"。

まず、保持するスナップショット コピーの数を指定するルールを含むSnapMirrorポリシーを作成する必要があります。

1. FSx クラスターにSnapMirrorポリシーを作成します。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. SnapCenterポリシーで指定されたセカンダリ ポリシー ラベルと一致するSnapMirrorラベルを使用して、ポリシーにルールを追加します。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy  
PolicyName -snapmirror-label SnapMirrorLabelName -keep  
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



各SnapMirrorラベルと保持するスナップショットの数 (保持期間) に対して追加のルールを作成します。

宛先ボリュームを作成する

ソース ボリュームからのスナップショット コピーの受信者となる FSx 上の宛先ボリュームを作成するには、FSx ONTAPで次のコマンドを実行します。

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームと宛先ボリューム間のSnapMirror関係を作成する

ソース ボリュームと宛先ボリュームの間にSnapMirror関係を作成するには、FSx ONTAPで次のコマンドを実行します。

```
FSx-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

SnapMirror関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソース ボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

オンプレミスで **Windows SnapCenter**サーバーを展開および構成します。

Windows SnapCenter Server をオンプレミスに導入

このソリューションは、NetApp SnapCenterを使用して、SQL Server および Oracle データベースのアプリケーション整合性のあるバックアップを取得します。仮想マシン VMDK をバックアップする Veeam Backup & Replication と組み合わせることで、オンプレミスおよびクラウドベースのデータセンター向けの包括的な災害復旧ソリューションが提供されます。

SnapCenter softwareはNetAppサポート サイトから入手でき、ドメインまたはワークグループ内に存在する Microsoft Windows システムにインストールできます。詳細な計画ガイドとインストール手順については、"[NetAppドキュメント センター](#)"。

SnapCenter softwareは以下から入手できます。"[このリンク](#)"。

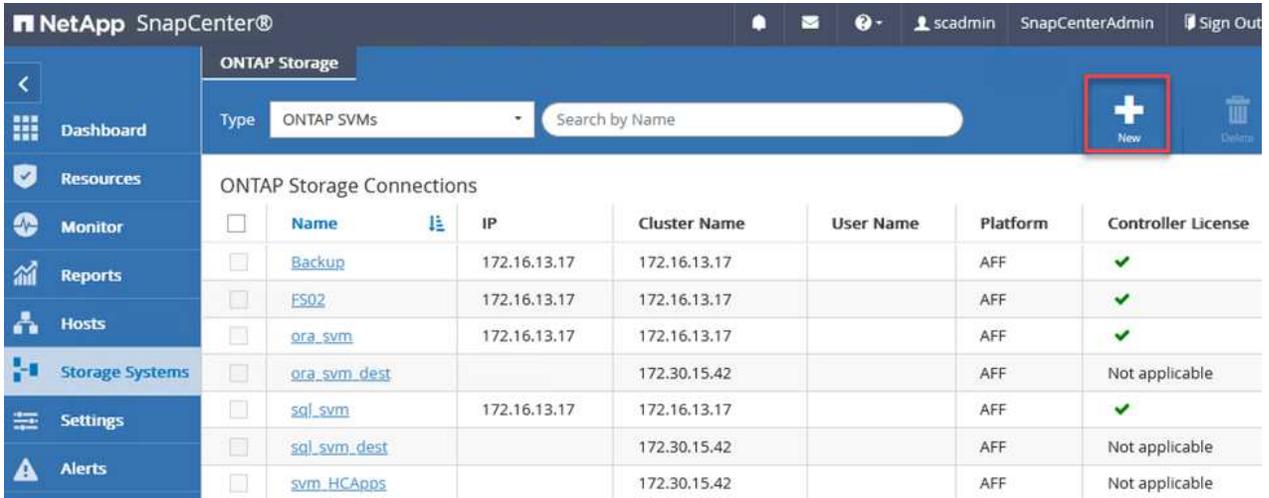
インストール後、https://Virtual_Cluster_IP_or_FQDN:8146 を使用して Web ブラウザーからSnapCenter コンソールにアクセスできるようになります。

コンソールにログインしたら、SQL Server および Oracle データベースのバックアップ用にSnapCenter を構成する必要があります。

SnapCenterにストレージコントローラを追加する

SnapCenterにストレージ コントローラを追加するには、次の手順を実行します。

1. 左側のメニューから [ストレージ システム] を選択し、[新規] をクリックして、ストレージ コントローラをSnapCenterに追加するプロセスを開始します。



The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes the NetApp logo, 'SnapCenter', and user information. The left sidebar contains a menu with options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'ONTAP Storage' and features a 'Type' dropdown set to 'ONTAP SVMs' and a search bar. A red box highlights a '+ New' button in the top right corner. Below this is a table of 'ONTAP Storage Connections' with columns for Name, IP, Cluster Name, User Name, Platform, and Controller License.

<input type="checkbox"/>	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	Backup	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	FS02	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	sql_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	svm_HCApps		172.30.15.42		AFF	Not applicable

2. [ストレージ システムの追加] ダイアログ ボックスで、ローカルのオンプレミスONTAPクラスターの管理 IP アドレスとユーザー名およびパスワードを追加します。次に、「送信」をクリックしてストレージ システムの検出を開始します。

Add Storage System

Add Storage System

Storage System	<input type="text" value="10.61.181.180"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="●●●●●●●●"/>

Event Management System (EMS) & AutoSupport Settings

- Send AutoSupport notification to storage system
- Log SnapCenter Server events to syslog
-  **More Options** : Platform, Protocol, Preferred IP etc..

- このプロセスを繰り返して、FSx ONTAPシステムをSnapCenterに追加します。この場合、「ストレージシステムの追加」ウィンドウの下部にある「その他のオプション」を選択し、「セカンダリ」のチェックボックスをクリックして、FSxシステムをSnapMirrorコピーまたはプライマリバックアップスナップショットで更新されたセカンダリストレージシステムとして指定します。

More Options



Platform FAS

Secondary 

Protocol HTTPS

Port 443

Timeout 60 seconds 

Preferred IP 

Save

Cancel

SnapCenterへのストレージシステムの追加に関する詳細については、次のドキュメントを参照してください。 ["このリンク"](#)。

SnapCenterにホストを追加する

次のステップは、ホスト アプリケーション サーバーをSnapCenterに追加することです。プロセスはSQL Server と Oracle の両方で同様です。

1. 左側のメニューから [ホスト] を選択し、[追加] をクリックして、SnapCenterにストレージ コントローラーを追加するプロセスを開始します。
2. [ホストの追加] ウィンドウで、ホスト タイプ、ホスト名、およびホスト システムの資格情報を追加します。プラグインの種類を選択します。SQL Server の場合は、Microsoft Windows および Microsoft SQL Server プラグインを選択します。

NetApp SnapCenter®

Managed Hosts

Search by Name

<input type="checkbox"/>	Name
<input type="checkbox"/>	oraclesrv_01.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_02.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_03.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_04.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_05.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_06.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_07.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_08.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_09.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_10.sddc.netapp.com

Add Host

Host Type: Windows

Host Name: sqlsrv-01.sddc.netapp.com

Credentials: sddc-jpowell

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Windows

- Microsoft Windows
- Microsoft SQL Server
- Microsoft Exchange Server
- SAP HANA

More Options : Port, gMSA, Install Path, Custom Plug-Ins...

Submit Cancel

3. Oracleの場合、「ホストの追加」ダイアログボックスの必須フィールドに入力し、Oracle Database プラグインのチェックボックスをオンにします。「送信」をクリックすると検出プロセスが開始され、ホストがSnapCenterに追加されます。

Add Host

Host Type

Host Name

Credentials



Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

Oracle Database

SAP HANA

 [More Options](#) : Port, Install Path, Custom Plug-Ins...

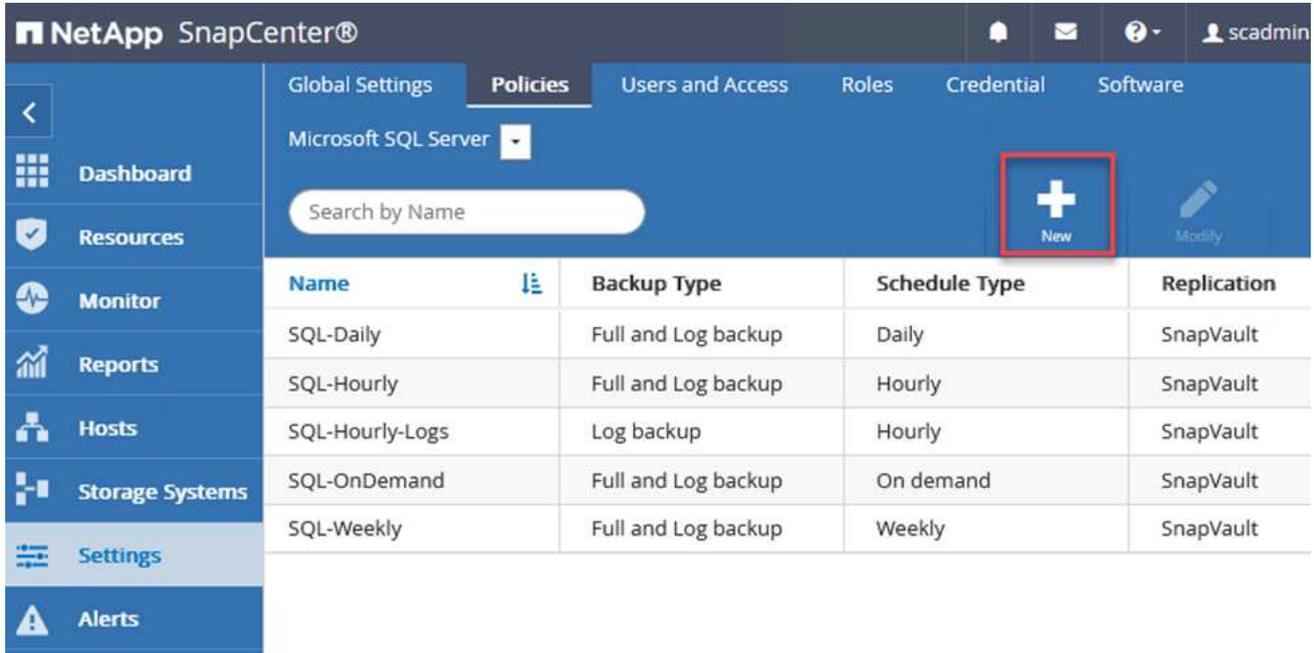
Submit

Cancel

SnapCenterポリシーを作成する

ポリシーは、バックアップ ジョブに従う特定のルールを確立します。これらには、バックアップ スケジュール、レプリケーション タイプ、SnapCenter がトランザクション ログのバックアップと切り捨てを処理する方法などが含まれますが、これらに限定されません。

SnapCenter Web クライアントの [設定] セクションでポリシーにアクセスできます。



The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes 'Global Settings', 'Policies', 'Users and Access', 'Roles', 'Credential', and 'Software'. The 'Policies' tab is selected, and the server type is set to 'Microsoft SQL Server'. A search bar labeled 'Search by Name' is present. A red box highlights the 'New' button (a plus sign icon) in the top right corner of the table area. Below the navigation bar is a table with the following data:

Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

SQL Serverバックアップのポリシー作成の詳細については、"[SnapCenterのドキュメント](#)"。

Oracleバックアップのポリシー作成の詳細については、"[SnapCenterのドキュメント](#)"。

注記:

- ポリシー作成ウィザードを進める際には、レプリケーション セクションに特に注意してください。このセクションでは、バックアップ プロセス中に取得するセカンダリSnapMirrorコピーの種類を指定します。
- 「ローカル Snapshot コピーの作成後にSnapMirrorを更新する」設定は、同じクラスタに存在する2つのストレージ仮想マシン間にSnapMirror関係が存在する場合に、その関係を更新することを指します。
- 「ローカル SnapShot コピーの作成後にSnapVault を更新する」設定は、2つの別個のクラスター間、およびオンプレミスのONTAPシステムとCloud Volumes ONTAPまたはFSx ONTAP間に存在するSnapMirror関係を更新するために使用されます。

次の画像は、上記のオプションと、それらがバックアップ ポリシー ウィザードでどのように表示されるかを示しています。

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

Error retry count

3

SnapCenterリソース グループを作成する

リソース グループを使用すると、バックアップに含めるデータベース リソースと、それらのリソースに適用するポリシーを選択できます。

1. 左側のメニューの「リソース」セクションに移動します。
2. ウィンドウの上部で、操作するリソース タイプ (この場合は Microsoft SQL Server) を選択し、[新しいリソース グループ] をクリックします。

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

SnapCenter のドキュメントでは、SQL Server と Oracle データベースの両方のリソース グループを作成する手順が詳細に説明されています。

SQLリソースをバックアップするには、["このリンク"](#)。

Oracleリソースのバックアップについては、["このリンク"](#)。

Veeam バックアップ サーバーの導入と構成

このソリューションでは、Veeam Backup & Replication ソフトウェアを使用してアプリケーション仮想マシンをバックアップし、Veeam スケールアウト バックアップ リポジトリ (SOBR) を使用してバックアップのコピーを Amazon S3 バケットにアーカイブします。このソリューションでは、Veeam は Windows サーバーに展開されます。Veeamの導入に関する具体的なガイダンスについては、"[Veeamヘルプセンター 技術ドキュメント](#)"。

Veeamスケールアウトバックアップリポジトリを構成する

ソフトウェアを展開してライセンスを取得したら、バックアップジョブのターゲットストレージとしてスケールアウトバックアップリポジトリ (SOBR) を作成できます。また、災害復旧のために VM データのオフサイトバックアップとして S3 バケットも含める必要があります。

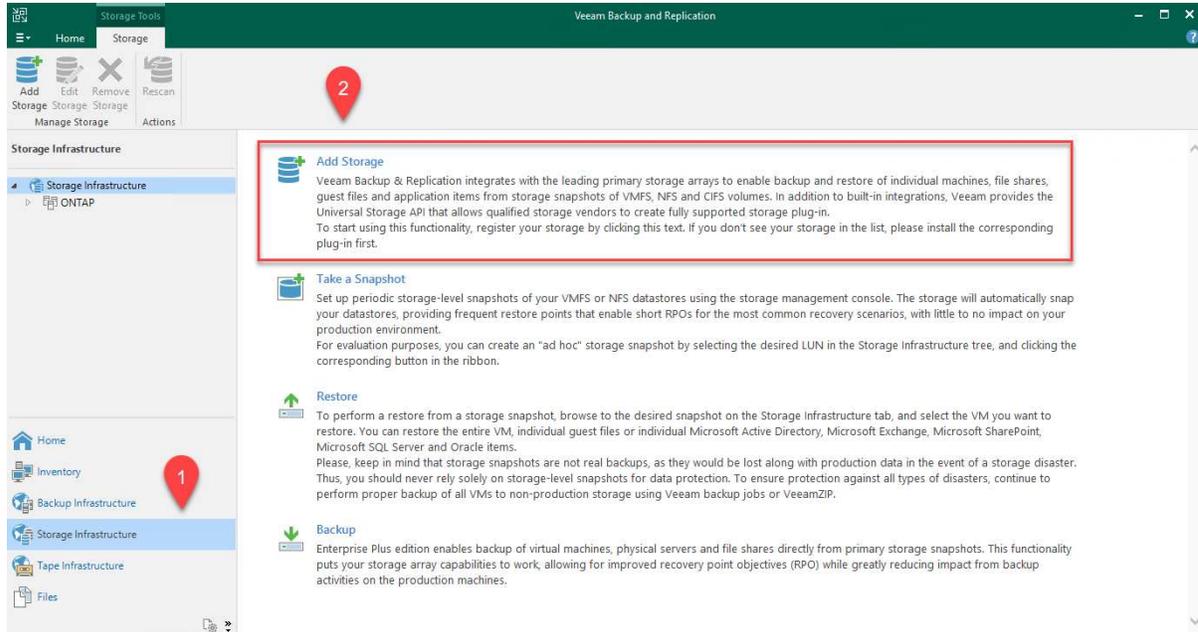
始める前に次の前提条件を確認してください。

1. オンプレミスのONTAPシステムに、バックアップのターゲットストレージとして SMB ファイル共有を作成します。
2. SOBR に含める Amazon S3 バケットを作成します。これはオフサイトバックアップのリポジトリです。

VeeamにONTAPストレージを追加

まず、ONTAPストレージ クラスターと関連する SMB/NFS ファイルシステムを Veeam のストレージ インフラストラクチャとして追加します。

1. Veeam コンソールを開いてログインします。「ストレージ インフラストラクチャ」に移動し、「ストレージの追加」を選択します。



2. ストレージの追加ウィザードで、ストレージ ベンダーとしてNetAppを選択し、Data ONTAPを選択します。
3. 管理 IP アドレスを入力し、NAS Filer ボックスをオンにします。[Next]をクリックします。

New NetApp Data ONTAP Storage



Name

Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
Credentials	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

< Previous **Next >** Finish Cancel

4. ONTAPクラスターにアクセスするための資格情報を追加します。

New NetApp Data ONTAP Storage



Credentials

Specify account with storage administrator privileges.

Name	Credentials: <input type="text" value="HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)"/>	<input type="button" value="Add..."/>
Credentials	Manage accounts	
NAS Filer	Protocol: <input type="text" value="HTTPS"/>	
Apply	Port: <input type="text" value="443"/>	
Summary		

< Previous **Next >** Finish Cancel

5. NAS Filer ページで、スキャンするプロトコルを選択し、「次へ」を選択します。

New NetApp Data ONTAP Storage ×

NAS Filer
Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:
Credentials	<input checked="" type="checkbox"/> SMB
NAS Filer	<input type="checkbox"/> NFS
Apply	<input checked="" type="checkbox"/> Create required export rules automatically
Summary	Volumes to scan:
	All volumes Choose...
	Backup proxies to use:
	Automatic selection Choose...

< Previous
Apply
Finish
Cancel

6. ウィザードの [適用] ページと [概要] ページを完了し、[完了] をクリックしてストレージ検出プロセスを開始します。スキャンが完了すると、ONTAPクラスターがNASファイラーとともに使用可能なリソースとして追加されます。

 Add Storage
Manage Storage

 Edit Storage

 Remove Storage

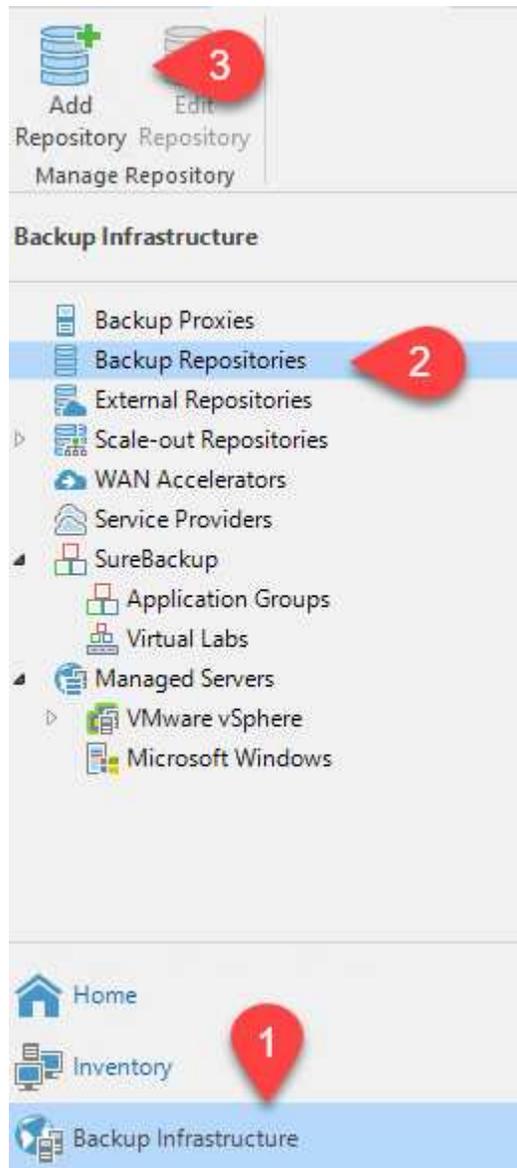
 Rescan
Actions

Storage Infrastructure

- Storage Infrastructure
 - ONTAP
 - E13A300
 - OTS-HC-Cluster
 - svm_nfs-A
 - svm0
 - iSCSI_Datastore
 - sqldb_vol2
 - sqldb_vol1
 - svm0_root

7. 新しく検出されたNAS共有を使用してバックアップリポジトリを作成します。バックアップインフラストラクチャから、バックアップリポジトリを選択し、リポジトリの追加メニュー項

目をクリックします。



8. 新しいバックアップ リポジトリ ウィザードのすべての手順に従ってリポジトリを作成します。Veeamバックアップリポジトリの作成の詳細については、"[Veeamのドキュメント](#)"。

New Backup Repository



Share

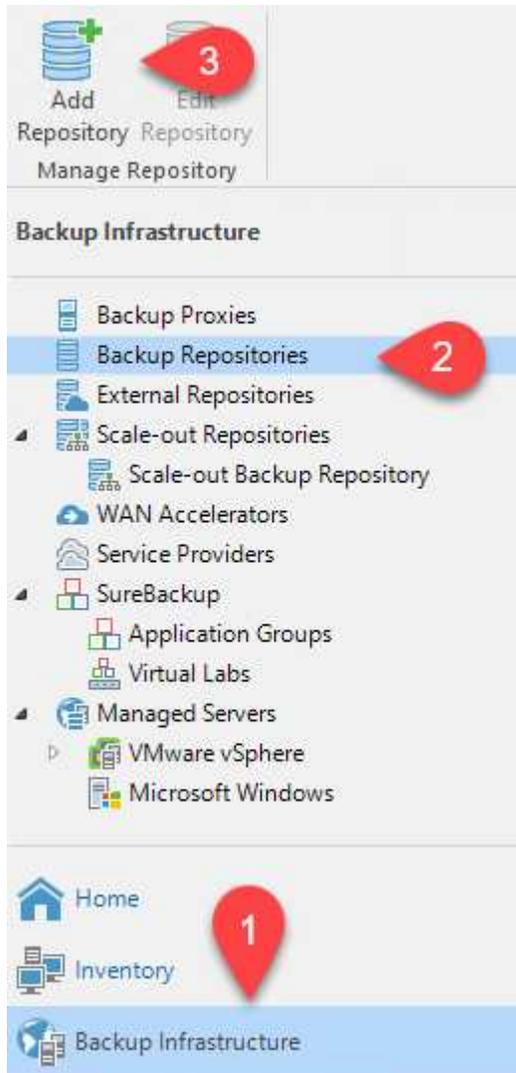
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name	Shared folder: <input type="text" value="\\172.21.162.181\VBRRepo"/> <input type="button" value="Browse..."/>
Share	<i>Use \\server\folder format</i>
Repository	<input checked="" type="checkbox"/> This share requires access credentials:
Mount Server	<input type="button" value="Key"/> sddc\administrator (sddc\administrator, last edited: 85 days ago) <input type="button" value="Add..."/>
Review	Manage accounts
Apply	Gateway server:
Summary	<input checked="" type="radio"/> Automatic selection
	<input type="radio"/> The following server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Use this option to improve performance and reliability of backup to a NAS located in a remote site.

Amazon S3 バケットをバックアップリポジトリとして追加する

次のステップは、Amazon S3 ストレージをバックアップリポジトリとして追加することです。

1. [バックアップ インフラストラクチャ] > [バックアップリポジトリ] に移動します。リポジトリの追加をクリックします。



2. バックアップリポジトリの追加ウィザードで、オブジェクトストレージを選択し、Amazon S3を選択します。これにより、新しいオブジェクトストレージリポジトリウィザードが起動します。

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

- オブジェクト ストレージ リポジトリの名前を指定して、「次へ」をクリックします。
- 次のセクションで、資格情報を入力します。AWS アクセスキーとシークレットキーが必要です。

New Object Storage Repository ×

 **Account**
Specify AWS account to use for connecting to Amazon S3 storage bucket.

Name	Credentials:
Account	<input type="text" value="AKIA4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add...
Bucket	Manage cloud accounts
Summary	AWS region: <input type="text" value="Global"/>

Use the following gateway server:

Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

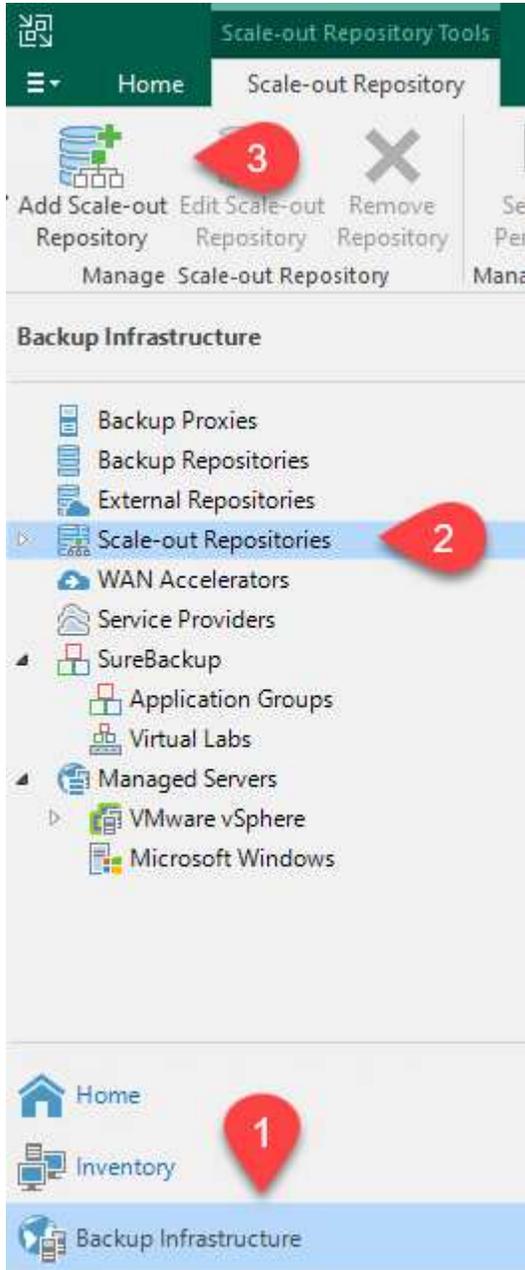
< Previous Next > Finish Cancel

- Amazon 構成が読み込まれたら、データセンター、バケット、フォルダーを選択し、「適用」をクリックします。最後に、「完了」をクリックしてウィザードを終了します。

スケールアウトバックアップリポジトリを作成する

ストレージリポジトリを Veeam に追加したので、災害復旧のためにオフサイトの Amazon S3 オブジェクトストレージにバックアップコピーを自動的に階層化する SOBR を作成できます。

1. バックアップインフラストラクチャから、スケールアウトリポジトリを選択し、スケールアウトリポジトリの追加メニュー項目をクリックします。



2. 新しいスケールアウトバックアップリポジトリで SOBR の名前を入力し、[次へ] をクリックします。
3. パフォーマンス層では、ローカルONTAPクラスタにある SMB 共有を含むバックアップリポジトリを選択します。

New Scale-out Backup Repository



Performance Tier

Select backup repositories to use as the landing zone and for the short-term retention.

Name	Extents:	
Performance Tier	Name	Add...
Placement Policy	VBRRepo2	Remove

4. 配置ポリシーでは、要件に基づいてデータのローカルリティまたはパフォーマンスのいずれかを選択します。次へを選択します。
5. 容量層では、Amazon S3 オブジェクト ストレージを使用して SOBR を拡張します。災害復旧のために、セカンダリ バックアップがタイムリーに配信されるように、[バックアップが作成されたらすぐにオブジェクト ストレージにコピーする]を選択します。

New Scale-out Backup Repository



Capacity Tier

Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

Name	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage:
Performance Tier	Amazon S3 Repo Add...
Placement Policy	Define time windows when uploading to capacity tier is allowed Window...
Capacity Tier	<input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.
Archive Tier	<input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.
Summary	Move backup files older than 14 days (your operational restore window) Override...
	<input type="checkbox"/> Encrypt data uploaded to object storage Password: Add... Manage passwords
<p>< Previous Next > Finish Cancel</p>	

6. 最後に、「適用」と「完了」を選択して、SOBR の作成を完了します。

スケールアウトバックアップリポジトリジョブを作成する

Veeam を構成する最後の手順は、新しく作成された SOBR をバックアップ先として使用してバックアップ ジョブを作成することです。バックアップ ジョブの作成は、ストレージ管理者の通常の業務の一部であるため、ここでは詳細な手順については説明しません。Veeamでのバックアップジョブ作成の詳細については、"[Veeamヘルプセンター技術ドキュメント](#)"。

BlueXP backup and recovery ツールと構成

AWS で実行されている VMware Cloud Volumes サービスへのアプリケーション VM とデータベース ボリュームのフェイルオーバーを実行するには、SnapCenter Server と Veeam Backup and Replication Server の両方の実行中のインスタンスをインストールして構成する必要があります。フェイルオーバーが完了したら、オンプレミスのデータセンターへのフェールバックが計画され実行されるまで、通常のバックアップ操作を再開するようにこれらのツールを構成する必要があります。

セカンダリ Windows SnapCenter Server を展開する

SnapCenter Server は、VMware Cloud SDDC にデプロイされるか、VMware Cloud 環境にネットワーク接続された VPC にある EC2 インスタンスにインストールされます。

SnapCenter softwareはNetAppサポート サイトから入手でき、ドメインまたはワークグループ内に存在する Microsoft Windows システムにインストールできます。詳細な計画ガイドとインストール手順については、"[NetAppドキュメント センター](#)"。

SnapCenter softwareは次の場所にあります。"[このリンク](#)"。

セカンダリ Windows SnapCenter Server を構成する

FSx ONTAPにミラーリングされたアプリケーション データの復元を実行するには、まずオンプレミスのSnapCenterデータベースの完全復元を実行する必要があります。このプロセスが完了すると、VM との通信が再確立され、FSx ONTAP をプライマリ ストレージとして使用してアプリケーションのバックアップを再開できるようになります。

これを実現するには、SnapCenterサーバーで次の項目を完了する必要があります。

1. コンピューター名を元のオンプレミスのSnapCenter Server と同じになるように構成します。
2. VMware Cloud および FSx ONTAPインスタンスと通信するためのネットワークを構成します。
3. SnapCenterデータベースを復元する手順を完了します。
4. SnapCenterがディザスタ リカバリ モードになっていることを確認して、FSx がバックアップのプライマリ ストレージになっていることを確認します。
5. 復元された仮想マシンとの通信が再確立されたことを確認します。

セカンダリVeeam Backup & Replicationサーバーを導入する

Veeam Backup & Replication サーバーは、VMware Cloud on AWS 内の Windows サーバーまたは EC2 インスタンスにインストールできます。詳細な実装ガイダンスについては、"[Veeamヘルプセンター技術ドキュメント](#)"。

セカンダリ Veeam Backup & Replication サーバーを構成する

Amazon S3 ストレージにバックアップされた仮想マシンの復元を実行するには、Windows サーバーに Veeam Server をインストールし、VMware Cloud、FSx ONTAP、および元のバックアップ リポジトリを含む S3 バケットと通信するように構成する必要があります。また、VM を復元した後に新しいバックアップを実行するには、FSx ONTAPに新しいバックアップ リポジトリを構成する必要があります。

このプロセスを実行するには、次の項目を完了する必要があります。

1. VMware Cloud、FSx ONTAP、および元のバックアップ リポジトリを含む S3 バケットと通信するようにネットワークを構成します。
2. FSx ONTAP上の SMB 共有を新しいバックアップ リポジトリとして構成します。
3. オンプレミスのスケールアウト バックアップ リポジトリの一部として使用されていた元の S3 バケットをマウントします。
4. VM を復元した後、SQL VM と Oracle VM を保護するための新しいバックアップ ジョブを確立します。

Veeamを使用したVMの復元の詳細については、セクションを参照してください。"[Veeam Full Restore でアプリケーション VM を復元する](#)"。

災害復旧のためのSnapCenterデータベースバックアップ

SnapCenter、災害発生時にSnapCenterサーバーを復旧できるように、基盤となる MySQL データベースと構成データのバックアップと復旧が可能です。私たちのソリューションでは、VPC にある AWS EC2 インスタンス上のSnapCenterデータベースと構成を復元しました。SnapCenterの災害復旧の詳細については、以下を参照してください。"[このリンク](#)"。

SnapCenterバックアップの前提条件

SnapCenterバックアップには次の前提条件が必要です。

- バックアップされたデータベースと構成ファイルを見つけるためにオンプレミスのONTAPシステム上に作成されたボリュームと SMB 共有。
- オンプレミスのONTAPシステムと AWS アカウントの FSx または CVO 間のSnapMirror関係。この関係は、バックアップされたSnapCenterデータベースと構成ファイルを含むスナップショットを転送するために使用されます。
- EC2 インスタンスまたは VMware Cloud SDDC 内の VM のいずれかのクラウド アカウントにインストールされた Windows Server。
- VMware Cloud の Windows EC2 インスタンスまたは VM にインストールされたSnapCenter。

SnapCenter のバックアップと復元プロセスの概要

- バックアップ db および構成ファイルをホストするためのボリュームをオンプレミスのONTAPシステムに作成します。
- オンプレミスと FSx/CVO の間にSnapMirror関係を設定します。
- SMB 共有をマウントします。
- API タスクを実行するための Swagger 認証トークンを取得します。
- db 復元プロセスを開始します。
- xcopy ユーティリティを使用して、db および config ファイルのローカル ディレクトリを SMB 共有にコピーします。
- FSx で、ONTAPボリュームのクローンを作成します (オンプレミスからSnapMirror経由でコピーされます)。
- FSx から EC2/VMware Cloud に SMB 共有をマウントします。
- 復元ディレクトリを SMB 共有からローカル ディレクトリにコピーします。
- Swagger から SQL Server の復元プロセスを実行します。

SnapCenterデータベースと構成をバックアップする

SnapCenter は、REST API コマンドを実行するための Web クライアント インターフェイスを提供します。Swaggerを介してREST APIにアクセスする方法については、SnapCenterのドキュメントを参照してください。 ["このリンク"](#)。

Swaggerにログインして認証トークンを取得する

Swagger ページに移動した後、データベース復元プロセスを開始するために認証トークンを取得する必要があります。

1. `https://< SnapCenter Server IP>:8146/swagger/` にある SnapCenter Swagger API Web ページにアクセスします。



Swagger

http://example.com/api Explore

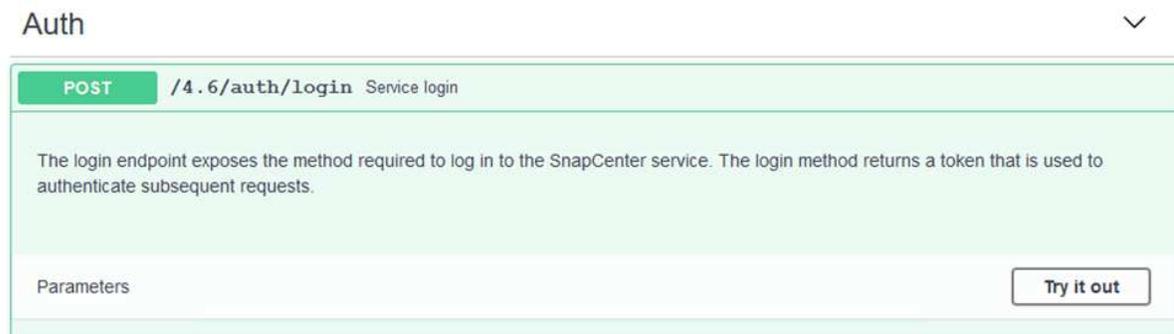
SnapCenter API

[Base URL: /api]

<https://snapcenter.sddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.
To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use
`https://{SCV_hostname}:{SCV_host_port}/api/swagger-ui.html`

2. 認証セクションを展開し、「試してみる」をクリックします。



Auth

POST /4.6/auth/login Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters

Try it out

3. UserOperationContext 領域で、SnapCenter の資格情報とロールを入力し、[実行] をクリックします。

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<input type="text" value="false"/>
UserOperationContext * required	User credentials
object (body)	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Edit Value Model</p> <pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre> </div> <p><input type="button" value="Cancel"/></p> <p>Parameter content type <input type="text" value="application/json"/></p> <p style="text-align: center;"><input type="button" value="Execute"/></p>

4. 以下のレスポンス本文でトークンを確認できます。バックアッププロセスを実行するときに、認証用のトークンテキストをコピーします。

```
200
Response body
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
"User": {
  "Token":
  "KlYxDq==tsV6E0dtdAmAYpe8q5SG6wcoGaSjwME6jrlNy5CsY63HRQ5LkoZLIESRNAhpGJJ00UQynEHdgtVGDZnvx+I/ZJZIn5M1NZrj6
  CLfGTApplGmcagT08bqb5kMfx07EcdraIdzAXUDb3Gy LOKtW0GdwKzSe0wKj3uVupnk1E31skK6FRBv9RS8j0qH0vo4v4RL0hhThhwFhV
  9/23nFeuJVP/p1Ev4vrV/ze2VTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjq==",
  "Name": "SCAdmin",
  "TokenBashed": null,
  "Type": "",
  "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
  "Id": "1",
  "FullName": "SCAdmin",
  "Host": null,
  "Author": null,
  "UserName": "",
  "Domain": "",
  "Passphrase": ""
}
```

SnapCenterデータベースのバックアップを実行する

次に、Swagger ページの Disaster Recovery 領域に移動して、SnapCenterバックアップ プロセスを開始します。

1. 災害復旧領域をクリックして展開します。

Disaster Recovery

- GET** /4.6/disasterrecovery/server/backup Fetch all the existing SnapCenter Server DR Backups.
- POST** /4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup.
- DELETE** /4.6/disasterrecovery/server/backup Deletes the existing Snapcenter DR backup.
- POST** /4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore.
- POST** /4.6/disasterrecovery/storage Enable or disable the storage disaster recovery.

2. 拡大する `/4.6/disasterrecovery/server/backup` セクションにアクセスし、[試してみる] をクリックします。

POST /4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters Try it out

3. SmDRBackupRequest セクションで、正しいローカル ターゲット パスを追加し、[実行] を選択してSnapCenterデータベースと構成のバックアップを開始します。

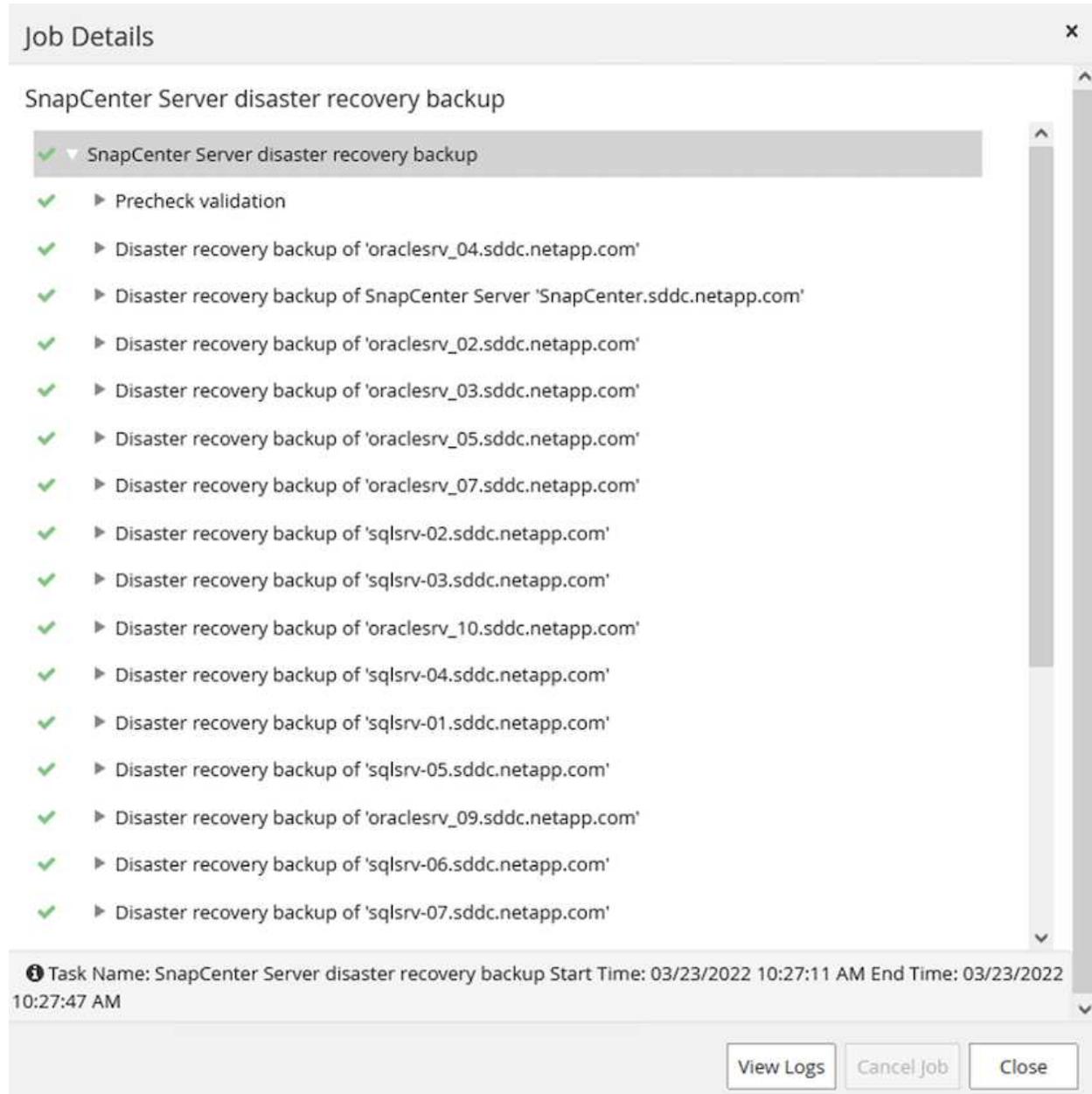


バックアップ プロセスでは、NFS または CIFS ファイル共有に直接バックアップすることはできません。

Name	Description
Token * required string (header)	User authorization token <input data-bbox="586 237 1027 279" type="text" value="TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ=="/>
SmDRBackupRequest * required object (body)	Parameters to take Backup <div data-bbox="581 384 1403 779"><p>Edit Value Model</p><pre data-bbox="597 426 984 478">{ "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }</pre></div> <div data-bbox="586 804 711 842"><input type="button" value="Cancel"/></div> <p>Parameter content type</p> <div data-bbox="586 894 885 930"><input type="text" value="application/json"/></div>

SnapCenterからバックアップジョブを監視する

データベースの復元プロセスを開始するときは、SnapCenterにログインしてログ ファイルを確認します。[モニター] セクションでは、SnapCenterサーバーの災害復旧バックアップの詳細を表示できます。



The screenshot shows a 'Job Details' window for a SnapCenter Server disaster recovery backup. The job is titled 'SnapCenter Server disaster recovery backup' and is marked as successful with a green checkmark. The job details list 15 sub-tasks, all of which are also marked as successful with green checkmarks. The sub-tasks include a precheck validation and 14 disaster recovery backups for various servers. At the bottom of the window, the task name, start time (03/23/2022 10:27:11 AM), and end time (03/23/2022 10:27:47 AM) are displayed. Three buttons are visible at the bottom right: 'View Logs', 'Cancel Job', and 'Close'.

Job Details [X]

SnapCenter Server disaster recovery backup

- ✓ SnapCenter Server disaster recovery backup
 - ✓ ▶ Precheck validation
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

i Task Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2022 10:27:47 AM

View Logs Cancel Job Close

XCOPYユーティリティを使用して、データベースのバックアップファイルを**SMB共有**にコピーします。

次に、SnapCenterサーバー上のローカルドライブから、AWSのFSxインスタンスにあるセカンダリロケーションにデータをSnapMirrorコピーするために使用されるCIFS共有にバックアップを移動する必要があります。ファイルの権限を保持する特定のオプションを指定してxcopyを使用します。

管理者としてコマンドプロンプトを開きます。コマンドプロンプトから次のコマンドを入力します。

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X  
/E /H /K  
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O  
/X /E /H /K
```

フェイルオーバー

プライマリサイトで災害が発生

プライマリオンプレミスデータセンターで災害が発生した場合、VMware Cloud on AWSを使用してAmazon Web Servicesインフラストラクチャにあるセカンダリサイトへのフェイルオーバーがシナリオに含まれます。仮想マシンとオンプレミスのONTAPクラスターにはアクセスできなくなっていると想定します。さらに、SnapCenterとVeeamの両方の仮想マシンにアクセスできなくなり、セカンダリサイトで再構築する必要があります。

このセクションでは、インフラストラクチャのクラウドへのフェイルオーバーについて説明し、次のトピックを取り上げます。

- SnapCenterデータベースの復元。新しいSnapCenterサーバーが確立されたら、MySQLデータベースと構成ファイルを復元し、データベースを災害復旧モードに切り替えて、セカンダリFSxストレージがプライマリストレージデバイスになることができますようにします。
- Veeam Backup & Replicationを使用してアプリケーション仮想マシンを復元します。VMバックアップが含まれているS3ストレージを接続し、バックアップをインポートして、VMware Cloud on AWSに復元します。
- SnapCenterを使用してSQL Serverアプリケーションデータを復元します。
- SnapCenterを使用してOracleアプリケーションデータを復元します。

SnapCenterデータベースの復元プロセス

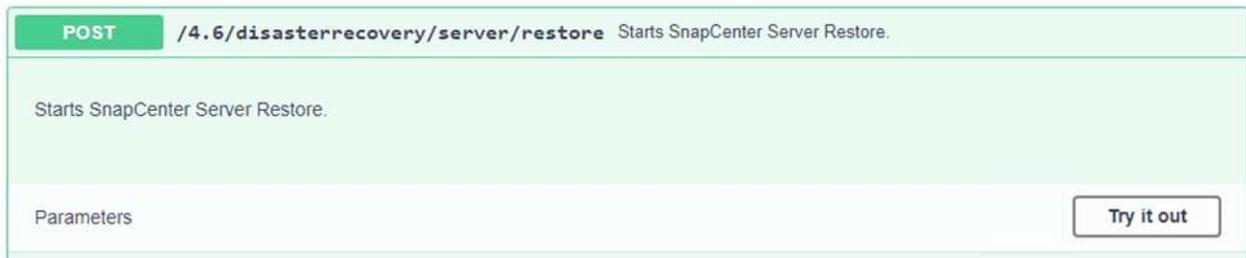
SnapCenter は、MySQL データベースと構成ファイルのバックアップと復元を可能にすることで、災害復旧シナリオをサポートします。これにより、管理者はオンプレミス データセンターでSnapCenterデータベースの定期的なバックアップを維持し、後でそのデータベースをセカンダリSnapCenterデータベースに復元できるようになります。

リモートSnapCenterサーバー上のSnapCenterバックアップ ファイルにアクセスするには、次の手順を実行します。

1. FSx クラスターからSnapMirror関係を解除し、ボリュームを読み取り/書き込み可能にします。
2. CIFS サーバーを作成し (必要な場合)、クローン ボリュームのジャンクション パスを指す CIFS 共有を作成します。
3. xcopy を使用して、バックアップ ファイルをセカンダリSnapCenterシステムのローカル ディレクトリにコピーします。
4. SnapCenter v4.6 をインストールします。
5. SnapCenterサーバーの FQDN が元のサーバーと同じであることを確認します。これは、DB の復元を成功させるために必要です。

復元プロセスを開始するには、次の手順を実行します。

1. セカンダリSnapCenterサーバーの Swagger API Web ページに移動し、前の手順に従って認証トークンを取得します。
2. Swaggerページの災害復旧セクションに移動し、`/4.6/disasterrecovery/server/restore`をクリックし、「試してみる」をクリックします。



3. 認証トークンを貼り付け、SmDRResterRequest セクションにバックアップの名前とセカンダリSnapCenterサーバー上のローカル ディレクトリを貼り付けます。

Name	Description
Token * required string (header)	User authorization token <input type="text" value="KIYxOg==rMXzS7EPIGRzTXJfton6Q+JoNGpueQt"/>
SmDRRestoreRequest * required object (body)	Parameters to take for Restore Edit Value Model <pre>{ "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\SnapCenter\\" }</pre>

4. 復元プロセスを開始するには、[実行] ボタンを選択します。
5. SnapCenterから [モニター] セクションに移動して、復元ジョブの進行状況を表示します。

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	🔄	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▼ SnapCenter Server Disaster Recovery
- ✓ ▼ Prepare for restore job
- ✓ ▼ Precheck validation
- ✓ ▼ Saving original server state
- ✓ ▼ Schedule restore
- ✓ ▼ Repository restore
- ✓ ▼ Config restore
- ✓ ▼ Reset MySQL password

6. セカンダリ ストレージからの SQL Server の復元を有効にするには、SnapCenterデータベースをデフォルトのリカバリ モードに切り替える必要があります。これは個別の操作として実行され、Swagger API Web ページで開始されます。
 - a. 災害復旧セクションに移動してクリックします /4.6/disasterrecovery/storage。
 - b. ユーザー認証トークンを貼り付けます。
 - c. SmSetDisasterRecoverySettingsRequestセクションで、変更します。
EnableDisasterRecover`に `true。
 - d. [実行] をクリックして、SQL Server の災害復旧モードを有効にします。

Name	Description
Token * required string (header)	User authorization token <input type="text" value="KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt"/>
SmSetDisasterRecoverySettingsRequest * required object (body)	Parameters to enable or disable the DR mode <div style="border: 1px solid #ccc; padding: 5px;">Edit Value Model <pre>{ "EnableDisasterRecovery": true }</pre></div>



追加の手順に関するコメントを参照してください。

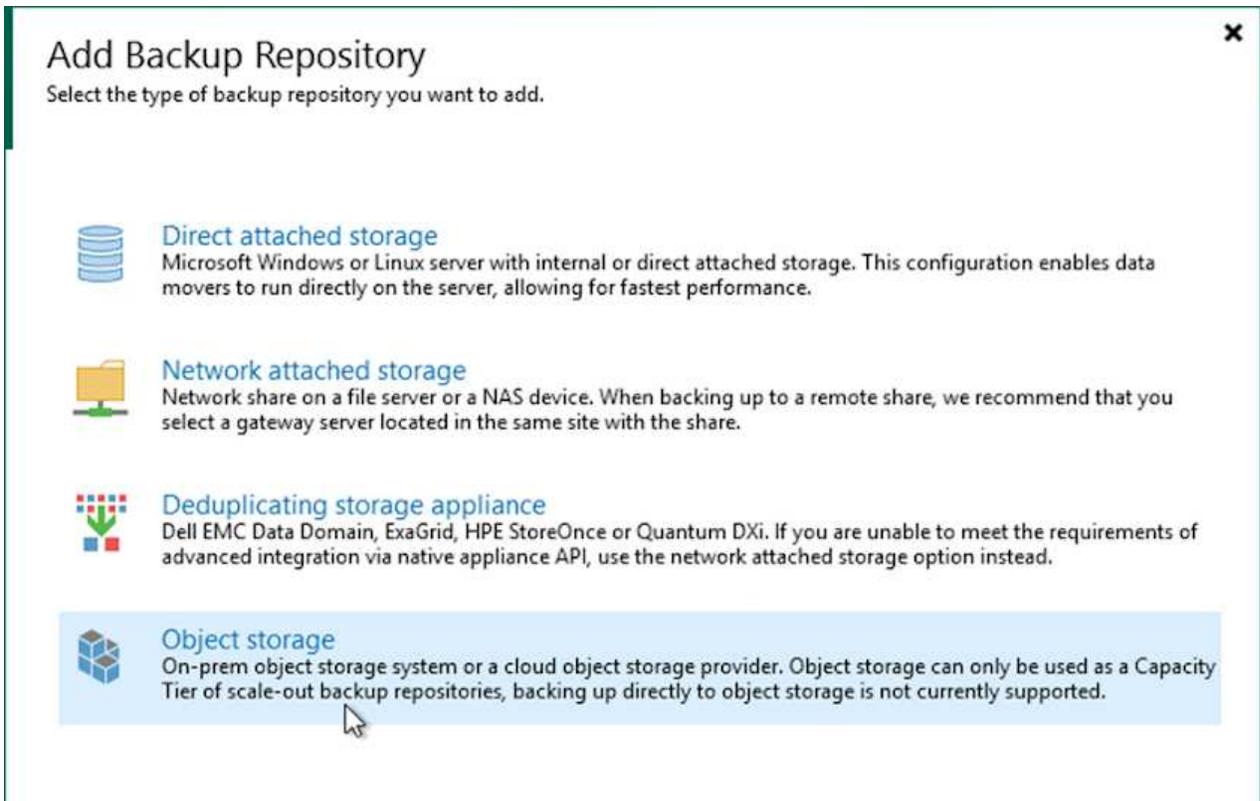
Veeam の完全復元でアプリケーション VM を復元する

バックアップリポジトリを作成し、S3からバックアップをインポートする

セカンダリ Veeam サーバーで、S3 ストレージからバックアップをインポートし、SQL Server および Oracle VM を VMware Cloud クラスタに復元します。

オンプレミスのスケールアウト バックアップ リポジトリの一部であった S3 オブジェクトからバックアップをインポートするには、次の手順を実行します。

1. [バックアップ リポジトリ] に移動し、上部のメニューで [リポジトリの追加] をクリックして、[バックアップ リポジトリの追加] ウィザードを起動します。ウィザードの最初のページで、バックアップ リポジトリの種類としてオブジェクト ストレージを選択します。



2. オブジェクトストレージタイプとして Amazon S3 を選択します。



Object Storage

Select the type of object storage you want to use as a backup repository.

-  **S3 Compatible**
Adds an on-premises object storage system or a cloud object storage provider.
-  **Amazon S3**
Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.
-  **Google Cloud Storage**
Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.
-  **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
-  **Microsoft Azure Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

3. Amazon クラウド ストレージ サービスのリストから、Amazon S3 を選択します。



Amazon Cloud Storage Services

Select the type of Amazon storage you want to use as a backup repository.

-  **Amazon S3**
Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.
-  **Amazon S3 Glacier**
Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.
-  **AWS Snowball Edge**
Adds AWS Snowball Edge appliance to enable seeding of backups into Amazon S3 object storage.

4. ドロップダウン リストから事前に入力した資格情報を選択するか、クラウド ストレージ リソースにアクセスするための新しい資格情報を追加します。「次へ」をクリックして続行します。

New Object Storage Repository ×

 **Account**
Specify AWS account to use for connecting to Amazon S3 storage bucket.

Name	Credentials:
Account	<input type="text" value="AKIA4H43ZT53YJXPY2Y (last edited: 33 days ago)"/> Add...
Bucket	Manage cloud accounts
Summary	AWS region: <input type="text" value="Global"/>

Use the following gateway server:

Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

< Previous Next > Finish Cancel

5. バケット ページで、データ センター、バケット、フォルダー、および必要なオプションを入力します。[Apply]をクリックします。

New Object Storage Repository ×

 **Bucket**
Specify Amazon S3 bucket to use.

Name	Data center: US East (N. Virginia) ▼
Account	Bucket: ehcveeamrepo Browse...
Bucket	Folder: RTP Browse...
Summary	<input type="checkbox"/> Limit object storage consumption to: 10 ▼ TB ▼ This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.
	<input type="checkbox"/> Make recent backups immutable for: 30 ▼ days Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.
	<input type="checkbox"/> Use infrequent access storage class (may result in higher costs) With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.
	<input type="checkbox"/> Store backups in a single availability zone (even lower price per GB, reduced resilience)

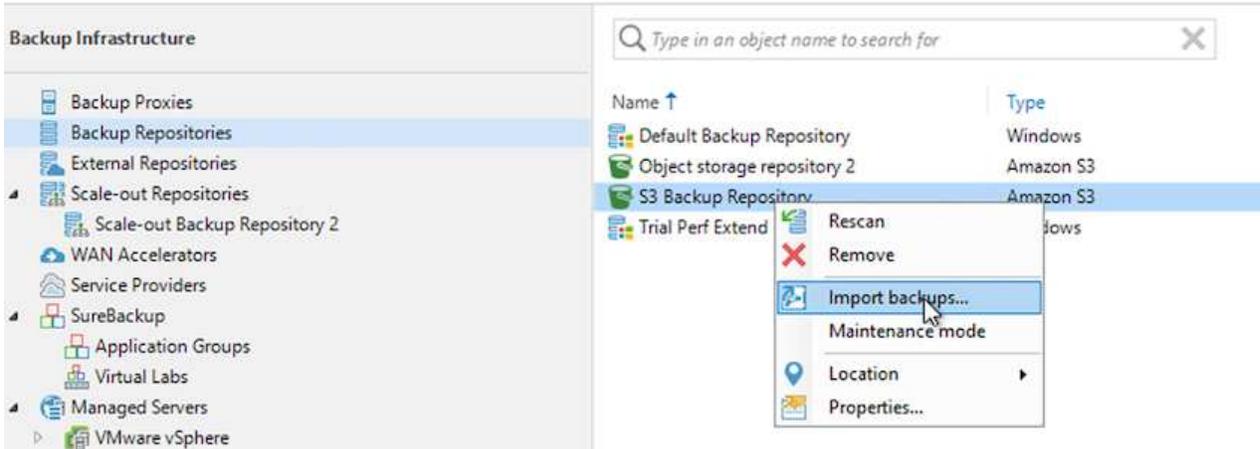
< Previous Apply Finish Cancel

- 最後に、「完了」を選択してプロセスを完了し、リポジトリを追加します。

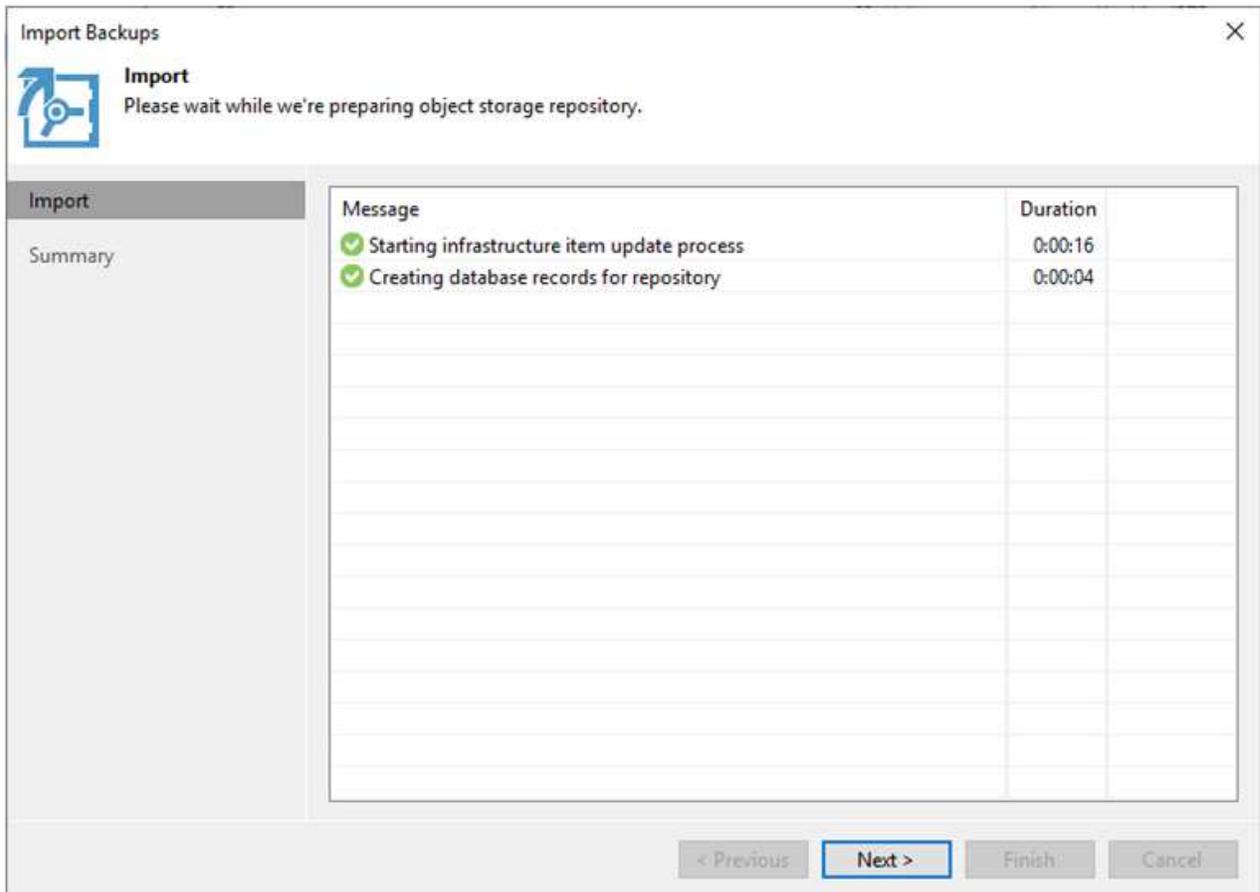
S3 オブジェクトストレージからバックアップをインポートする

前のセクションで追加した S3 リポジトリからバックアップをインポートするには、次の手順を実行します。

1. S3 バックアップ リポジトリから、[バックアップのインポート] を選択して、[バックアップのインポート] ウィザードを起動します。



2. インポート用のデータベース レコードが作成されたら、概要画面で [次へ] を選択し、[完了] を選択してインポート プロセスを開始します。



3. インポートが完了したら、VM を VMware Cloud クラスタに復元できます。

System



Name: **Configuration Database Resynchr...** Status: **Success**
Action type: Configuration Resynchronize Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\admin End time: 4/6/2022 3:04:57 PM

Log

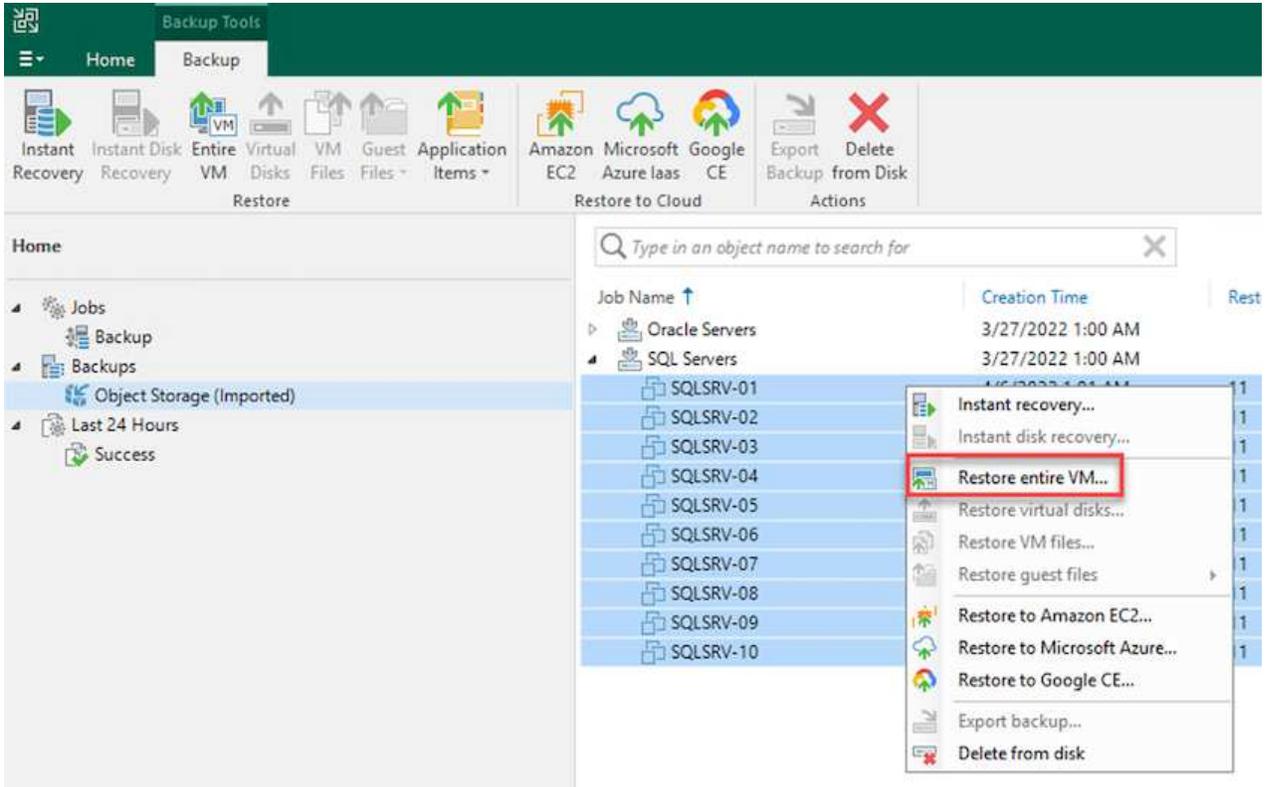
Message	Duration
✔ Starting backup repositories synchronization	
✔ Enumerating repositories	
✔ Found 1 repository	
✔ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✔ S3 Backup Repository: added 2 unencrypted	0:03:20
✔ Importing backup 2 out of 2	0:03:15
✔ Backup repositories synchronization completed successfully	

Close

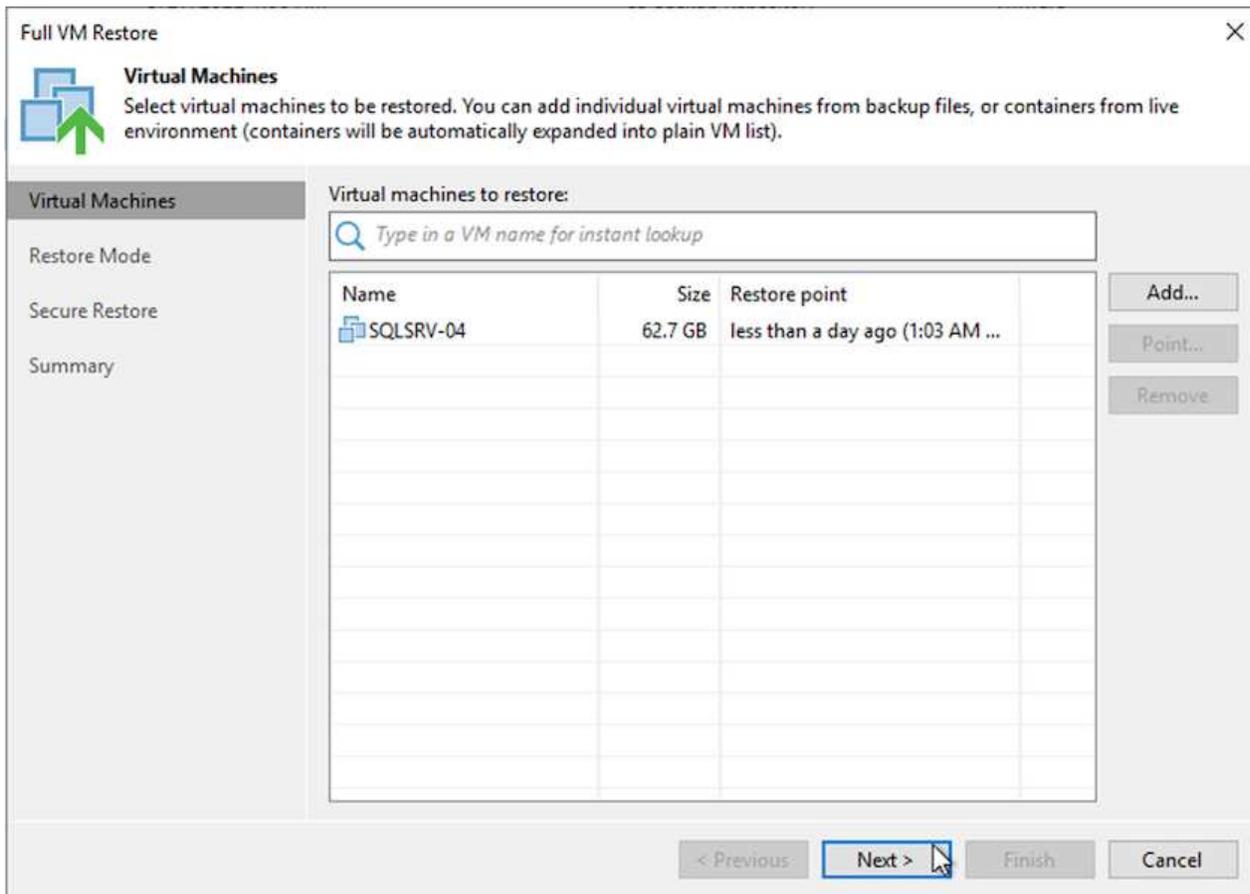
Veeam の完全リストアを使用してアプリケーション VM を VMware Cloud にリストアする

SQL および Oracle 仮想マシンを VMware Cloud on AWS ワークロード ドメイン/クラスタに復元するには、次の手順を実行します。

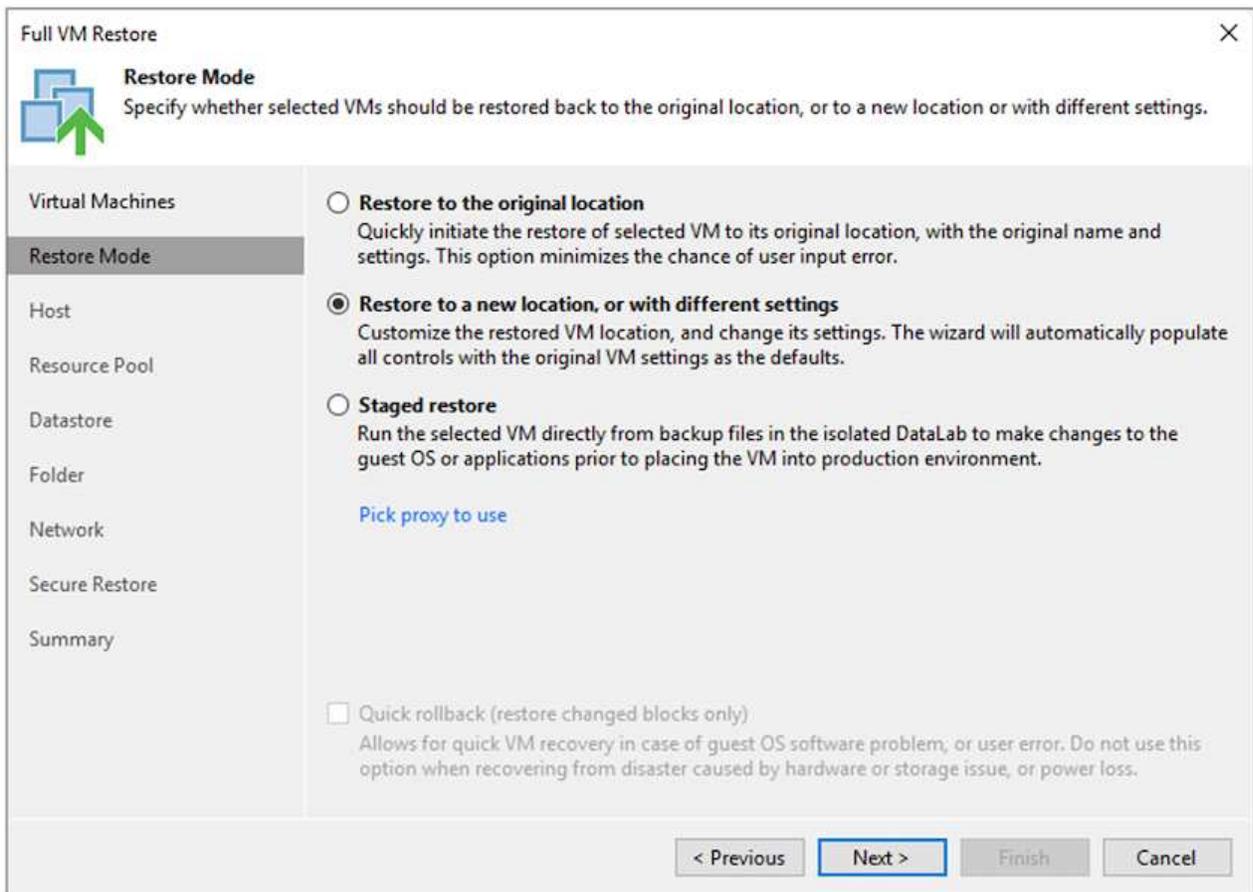
1. Veeam ホーム ページで、インポートされたバックアップを含むオブジェクト ストレージを選択し、復元する VM を選択して、右クリックし、[VM 全体の復元] を選択します。



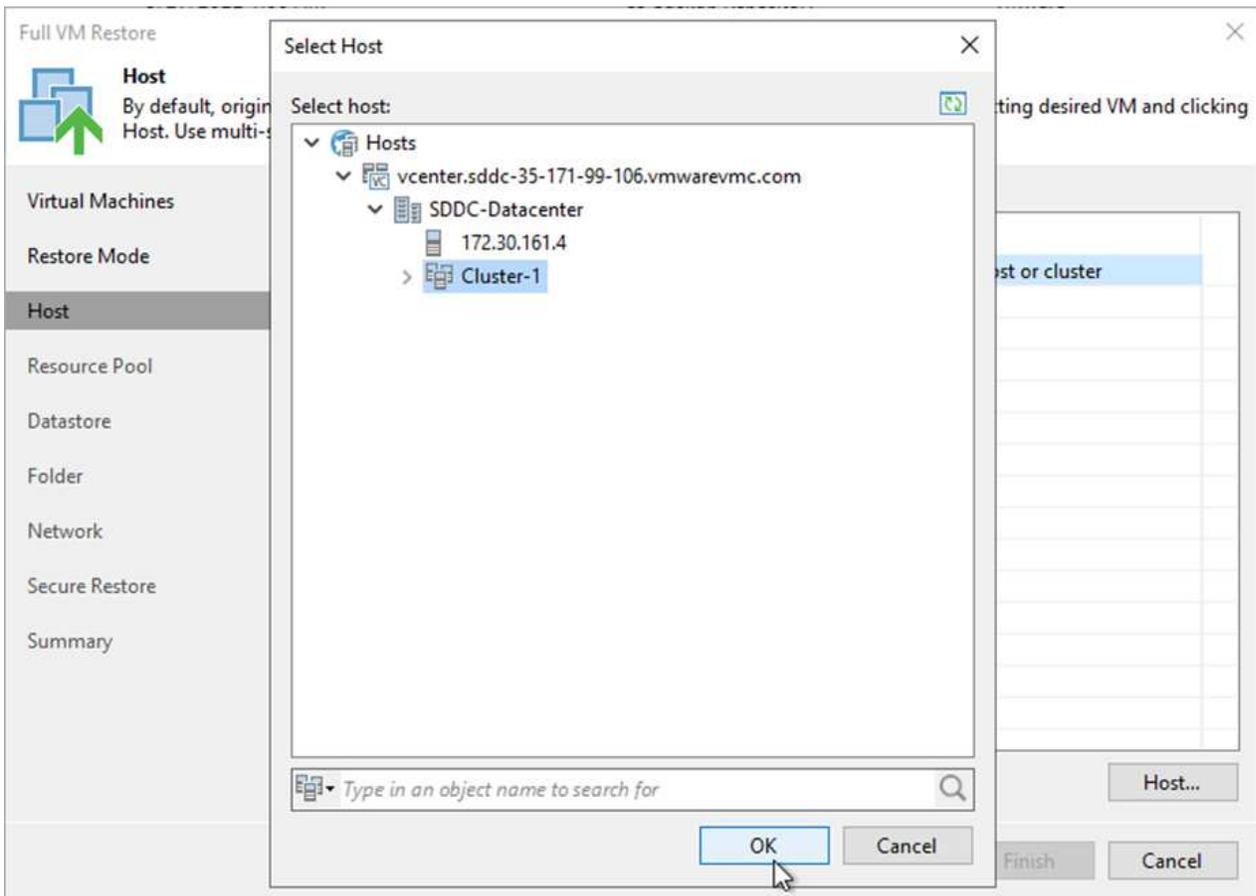
2. 完全な VM の復元ウィザードの最初のページで、必要に応じてバックアップする VM を変更し、[次へ] を選択します。



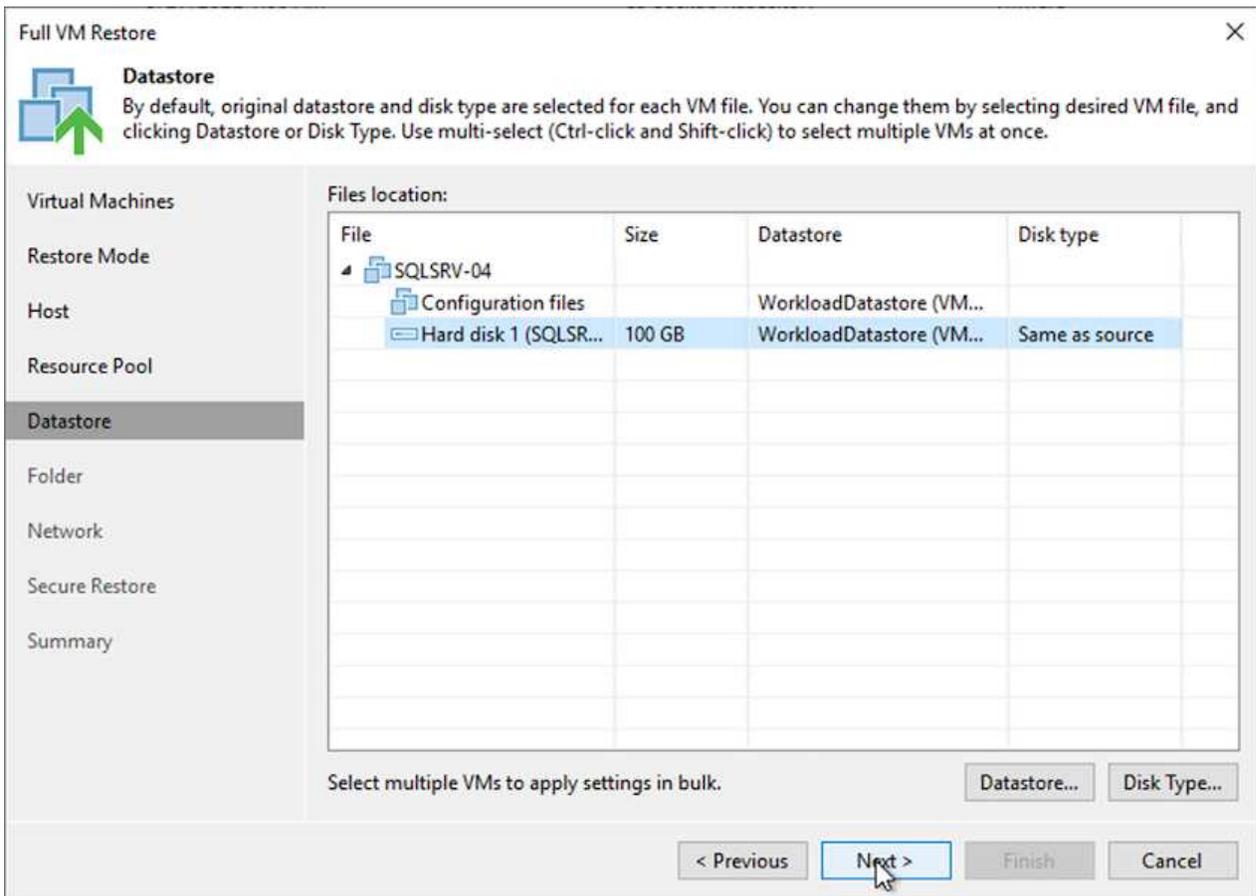
3. [復元モード] ページで、[新しい場所に復元] または [異なる設定で復元] を選択します。



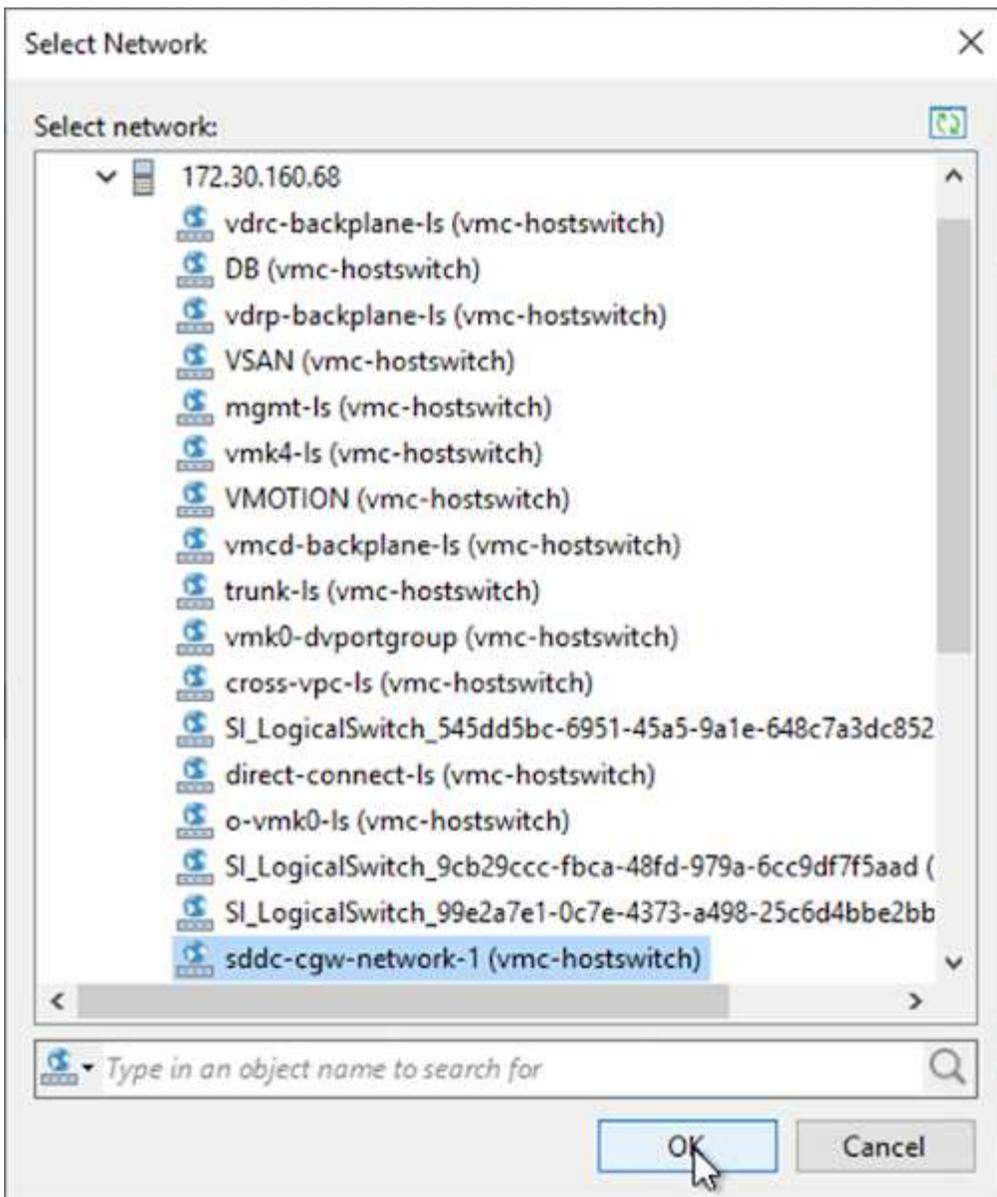
4. ホスト ページで、VM を復元するターゲット ESXi ホストまたはクラスターを選択します。



5. [データストア] ページで、構成ファイルとハード ディスクの両方のターゲット データストアの場所を選択します。



- [ネットワーク] ページで、VM 上の元のネットワークを新しいターゲットの場所のネットワークにマップします。



7. 復元された VM をマルウェアスキャンするかどうかを選択し、概要ページを確認して、[完了] をクリックして復元を開始します。

SQL Server アプリケーション データを復元する

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で SQL Server を復旧する方法について説明します。

回復手順を続行するには、次の前提条件が完了している必要があります。

1. Windows Server VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリ SnapCenter サーバーが確立され、SnapCenter データベースの復元と構成が、セクションに記載されている手順を使用して完了しました。"[SnapCenter のバックアップおよび復元プロセスの概要。](#)"

VM: SQL Server VM の復元後の構成

VM の復元が完了したら、SnapCenter内でホスト VM を再検出する準備として、ネットワークなどの項目を構成する必要があります。

1. 管理および iSCSI または NFS に新しい IP アドレスを割り当てます。
2. ホストを Windows ドメインに参加させます。
3. ホスト名を DNS または SnapCenter サーバー上のホスト ファイルに追加します。



SnapCenter プラグインが現在のドメインとは異なるドメイン資格情報を使用して展開された場合は、SQL Server VM 上の Windows 用プラグイン サービスのログオン アカウントを変更する必要があります。ログオン アカウントを変更した後、SnapCenter SMCORE、Plug-in for Windows、および Plug-in for SQL Server サービスを再起動します。



SnapCenter で復元された VM を自動的に再検出するには、FQDN がオンプレミスの SnapCenter に最初に追加された VM と同一である必要があります。

SQL Server の復元用に FSx ストレージを構成する

SQL Server VM の災害復旧復元プロセスを実行するには、FSx クラスターから既存の SnapMirror 関係を解除し、ボリュームへのアクセスを許可する必要があります。そのためには、次の手順を実行します。

1. SQL Server データベースとログ ボリュームの既存の SnapMirror 関係を解除するには、FSx CLI から次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VM の iSCSI IQN を含むイニシエーター グループを作成して、LUN へのアクセスを許可します。

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName  
-protocol iSCSI -ostype windows -initiator IQN
```

3. 最後に、作成したイニシエーター グループに LUN をマップします。

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup  
igroupName
```

4. パス名を見つけるには、`lun show` 指示。

Windows VMをiSCSIアクセス用にセットアップし、ファイルシステムを検出する

1. SQL Server VM から、FSx インスタンス上の iSCSI ターゲット インターフェイスへの接続が確立された VMware ポート グループで通信するように iSCSI ネットワーク アダプターを設定します。
2. iSCSI イニシエーターのプロパティ ユーティリティを開き、[検出]、[お気に入りのターゲット]、および [ターゲット] タブの古い接続設定をクリアします。
3. FSx インスタンス/クラスター上の iSCSI 論理インターフェイスにアクセスするための IP アドレスを見つけます。これは、AWS コンソールの Amazon FSx > ONTAP > Storage Virtual Machines にあります。

Endpoints

Management DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com 

NFS DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com 

iSCSI DNS name

iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com 

Management IP address

198.19.254.53 

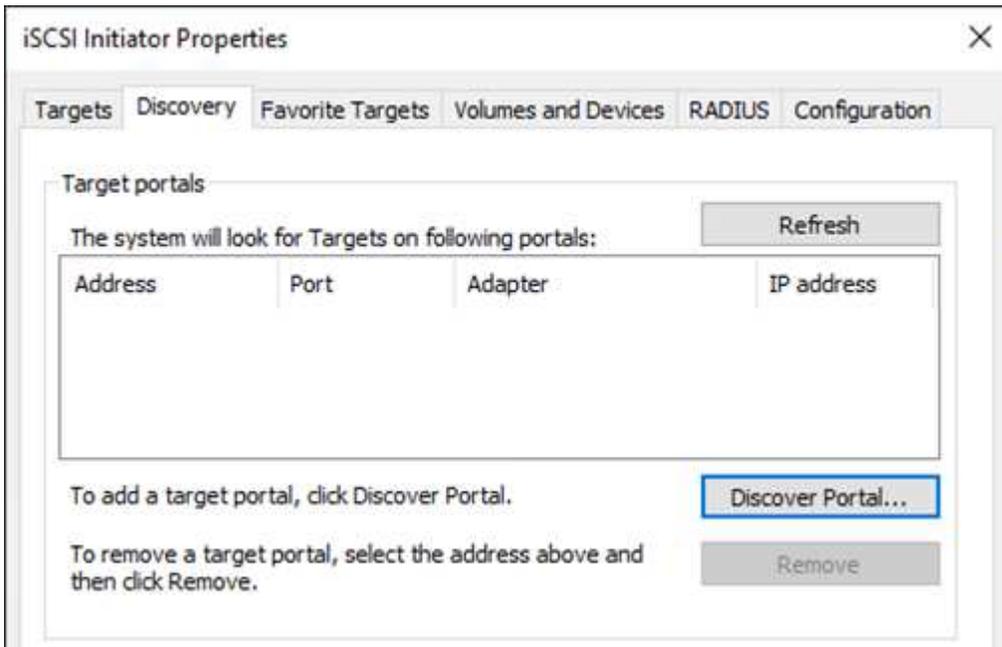
NFS IP address

198.19.254.53 

iSCSI IP addresses

172.30.15.101, 172.30.14.49 

4. [検出] タブから [ポータルの検出] をクリックし、FSx iSCSI ターゲットの IP アドレスを入力します。



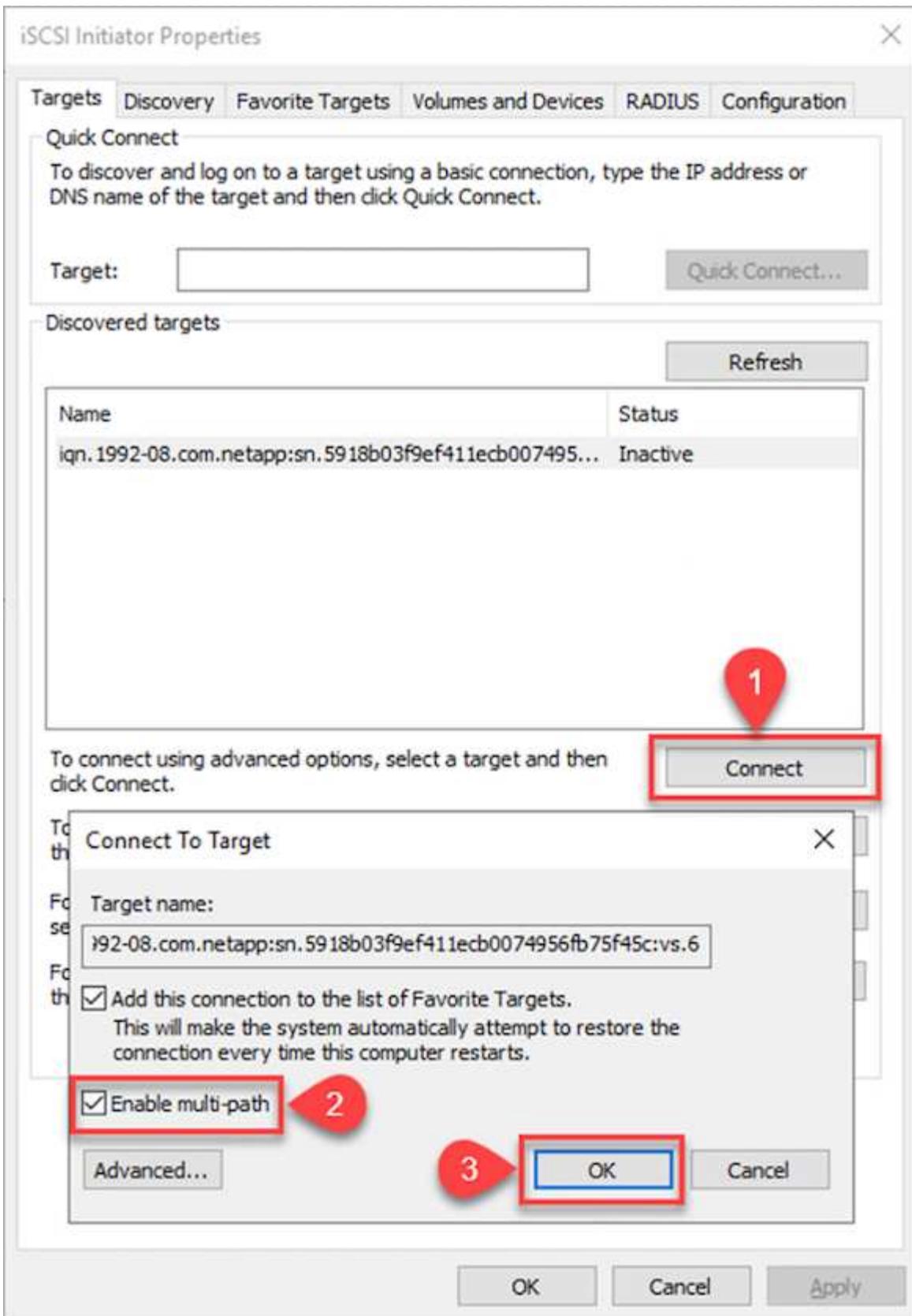
Discover Target Portal ✕

Enter the IP address or DNS name and port number of the portal you want to add.

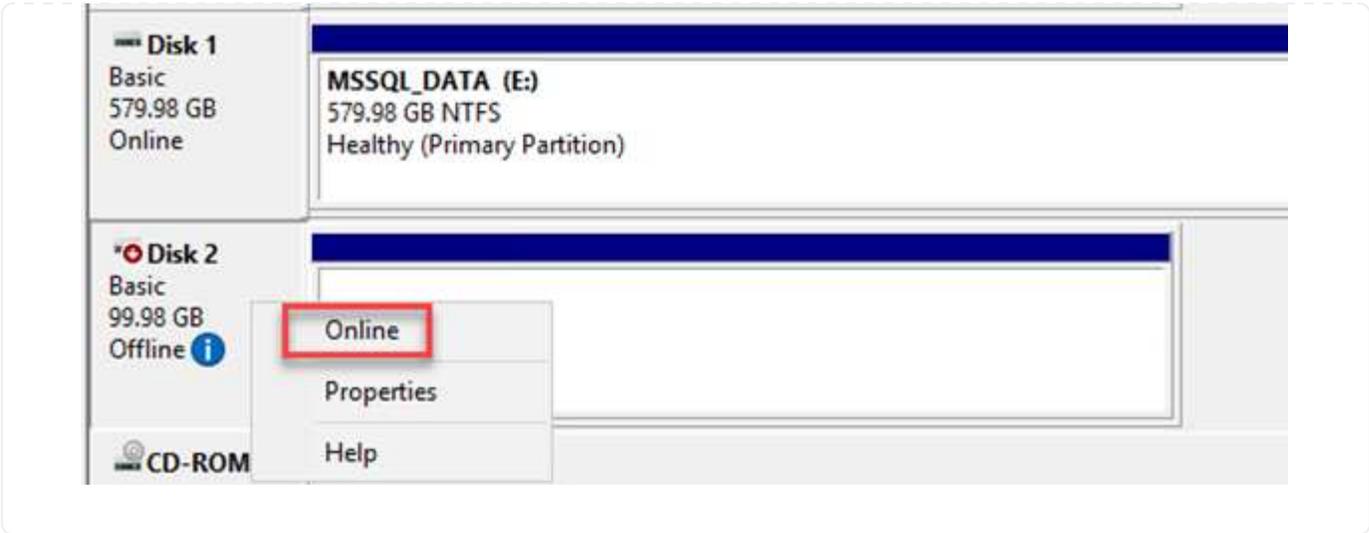
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: Port: (Default is 3260.)

5. [ターゲット] タブで [接続] をクリックし、構成に応じて [マルチパスを有効にする] を選択してから [OK] をクリックし、ターゲットに接続します。

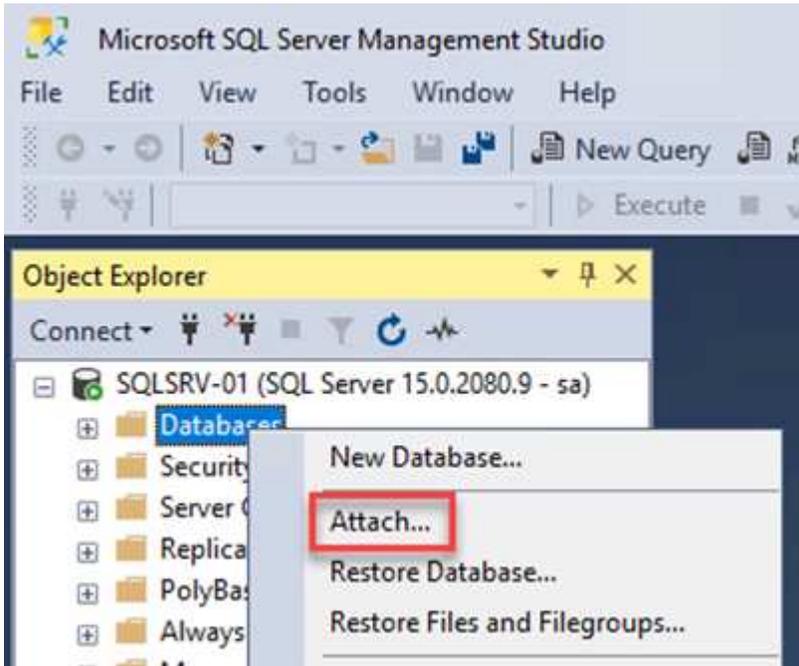


6. コンピュータの管理ユーティリティを開き、ディスクをオンラインにします。以前と同じドライブ文字が保持されていることを確認します。

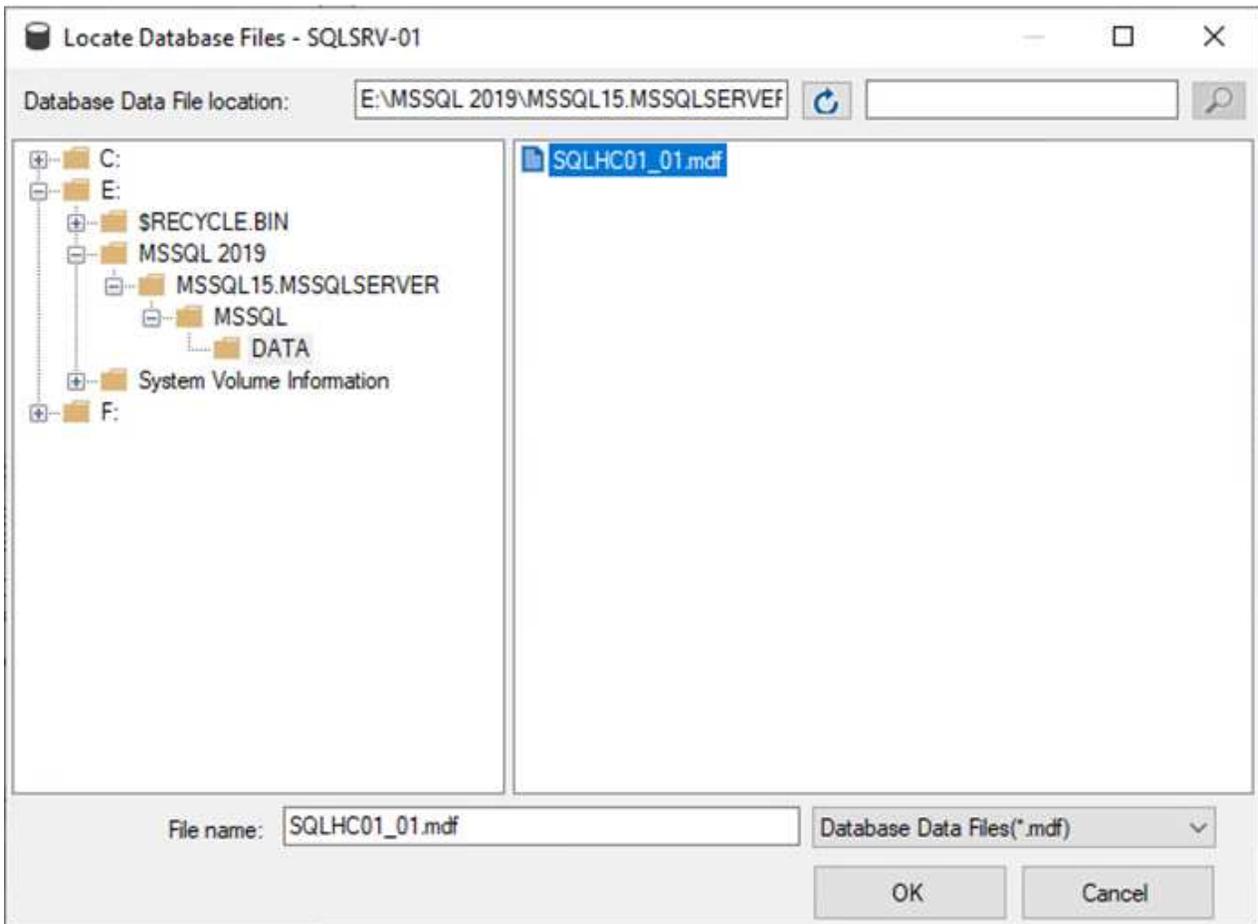


SQL Serverデータベースを接続する

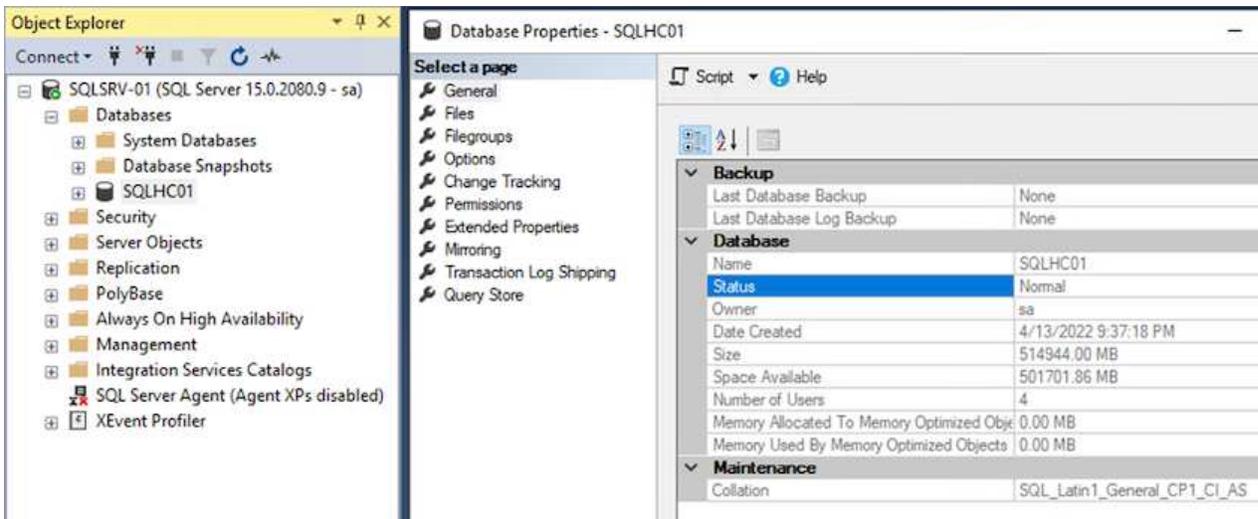
1. SQL Server VM から Microsoft SQL Server Management Studio を開き、[アタッチ] を選択してデータベースへの接続プロセスを開始します。



2. [追加] をクリックし、SQL Server プライマリ データベース ファイルが含まれているフォルダーに移動して選択し、[OK] をクリックします。



3. トランザクション ログが別のドライブにある場合は、トランザクション ログが含まれているフォルダーを選択します。
4. 完了したら、「OK」をクリックしてデータベースを接続します。

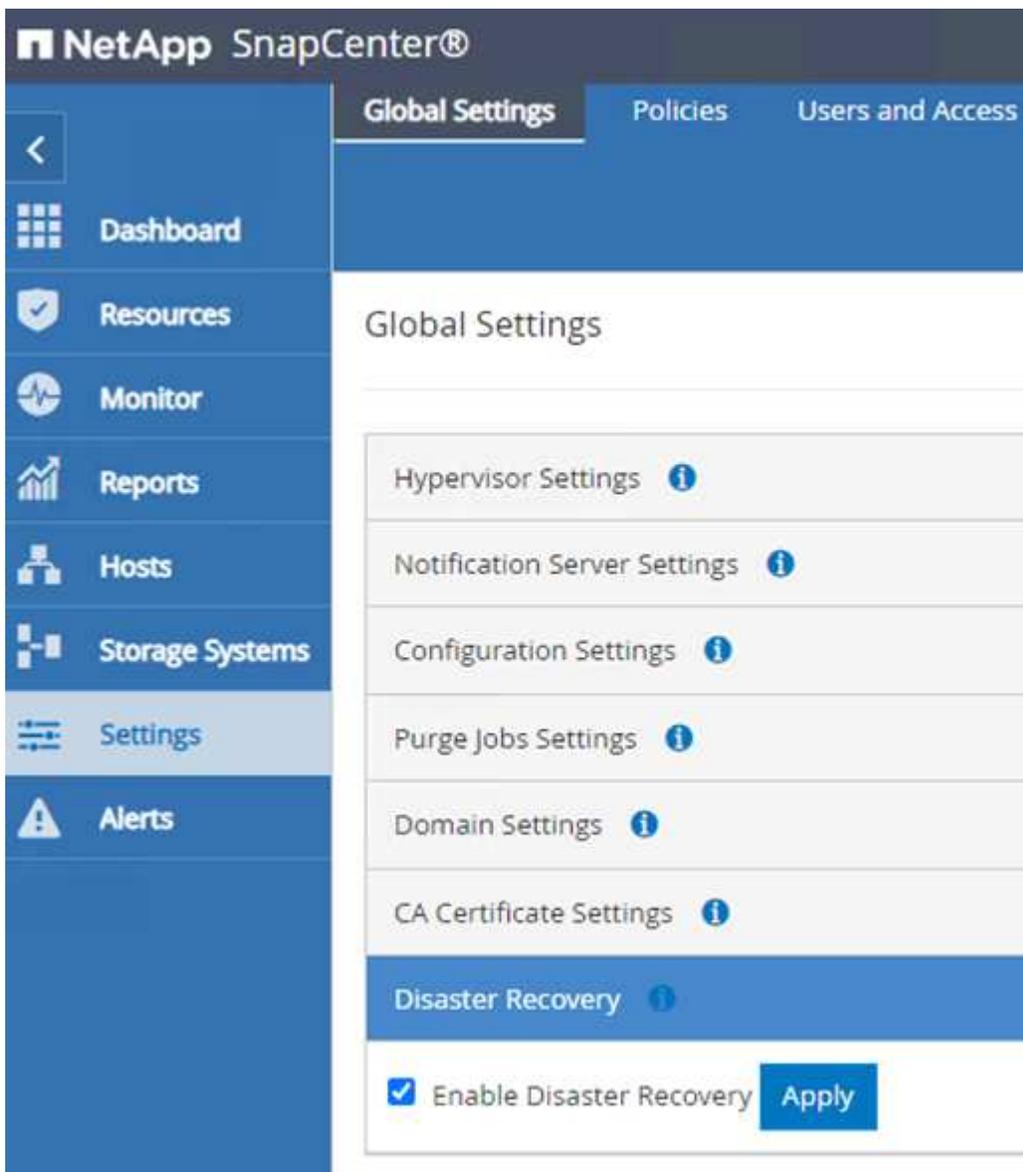


SnapCenterと SQL Server プラグインの通信を確認する

SnapCenterデータベースが以前の状態に復元されると、SQL Server ホストが自動的に再検出されます。これが正しく機能するには、次の前提条件に留意してください。

- SnapCenter を災害復旧モードにする必要があります。これは、Swagger API または災害復旧のグローバル設定を通じて実行できます。
- SQL Server の FQDN は、オンプレミスのデータセンターで実行されていたインスタンスと同一である必要があります。
- 元のSnapMirror関係を解除する必要があります。
- データベースを含む LUN は、SQL Server インスタンスにマウントされ、データベースが接続されている必要があります。

SnapCenterが災害復旧モードになっていることを確認するには、SnapCenter Web クライアント内から [設定] に移動します。[グローバル設定] タブに移動し、[災害復旧] をクリックします。「災害復旧を有効にする」チェックボックスが有効になっていることを確認します。



The screenshot shows the NetApp SnapCenter web interface. The top navigation bar includes 'Global Settings', 'Policies', and 'Users and Access'. The left sidebar contains a menu with 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'. The 'Settings' menu item is highlighted. The main content area is titled 'Global Settings' and lists several configuration categories: 'Hypervisor Settings', 'Notification Server Settings', 'Configuration Settings', 'Purge Jobs Settings', 'Domain Settings', 'CA Certificate Settings', and 'Disaster Recovery'. The 'Disaster Recovery' section is highlighted in blue and contains a checked checkbox labeled 'Enable Disaster Recovery' and an 'Apply' button.

Oracleアプリケーションデータの復元

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で Oracle アプリケーション データを復旧する方法について説明します。

回復手順を続行するには、次の前提条件を完了してください。

1. Oracle Linux サーバー VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリ SnapCenterサーバーが確立され、このセクションで概説されている手順を使用して SnapCenter データベースと構成ファイルが復元されました。"[SnapCenter のバックアップおよび復元プロセスの概要。](#)"

FSx for Oracle の復元を構成する – SnapMirror関係を解除する

FSx ONTAPインスタンスでホストされているセカンダリストレージボリュームを Oracle サーバーからアクセスできるようにするには、まず既存のSnapMirror関係を解除する必要があります。

1. FSx CLI にログインした後、次のコマンドを実行して、正しい名前でもフィルタリングされたボリュームを表示します。

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver      Volume          Aggregate      State      Type      Size      Available  Used%
-----
ora_svm_dest
  oraclesrv_03_u01_dest
    aggr1      online     DP        100GB     93.12GB   6%
ora_svm_dest
  oraclesrv_03_u02_dest
    aggr1      online     DP        200GB     34.98GB   82%
ora_svm_dest
  oraclesrv_03_u03_dest
    aggr1      online     DP        150GB     33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::> █
```

2. 既存のSnapMirror関係を解除するには、次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSxウェブクライアントでジャンクションパスを更新します。

oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0)

Attach

Actions ▲

Update volume

Create backup

Delete volume

Summary

Volume ID

fsvol-01167370e9b7aefa0 

Volume name

oraclesrv_03_u01_dest 

UUID

3d7338ce-9f19-11ec-
b007-4956fb75f45c

File system ID

fs-0ae40e08acc0dea67 

Resource ARN

arn:aws:fsx:us-
east-1:541696183547:volume/fs-
0ae40e08acc0dea67/fsvol-
01167370e9b7aefa0 

Creation time

2022-03-08T14:52:09-05:00

Lifecycle state

 Created

Volume type

ONTAP

Size

100.00 GB 

SVM ID

svm-02b2ad25c6b2e5bc2

Junction path

- 

Tiering policy name

SNAPSHOT_ONLY

Tiering policy cooling period (days)

2

Storage efficiency enabled

Disabled

4. ジャンクションパス名を追加し、[更新] をクリックします。Oracle サーバーから NFS ボリュームをマウントするときに、このジャンクションパスを指定します。

Update volume



Junction path

The location within your file system where your volume will be mounted.

Volume size



Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.



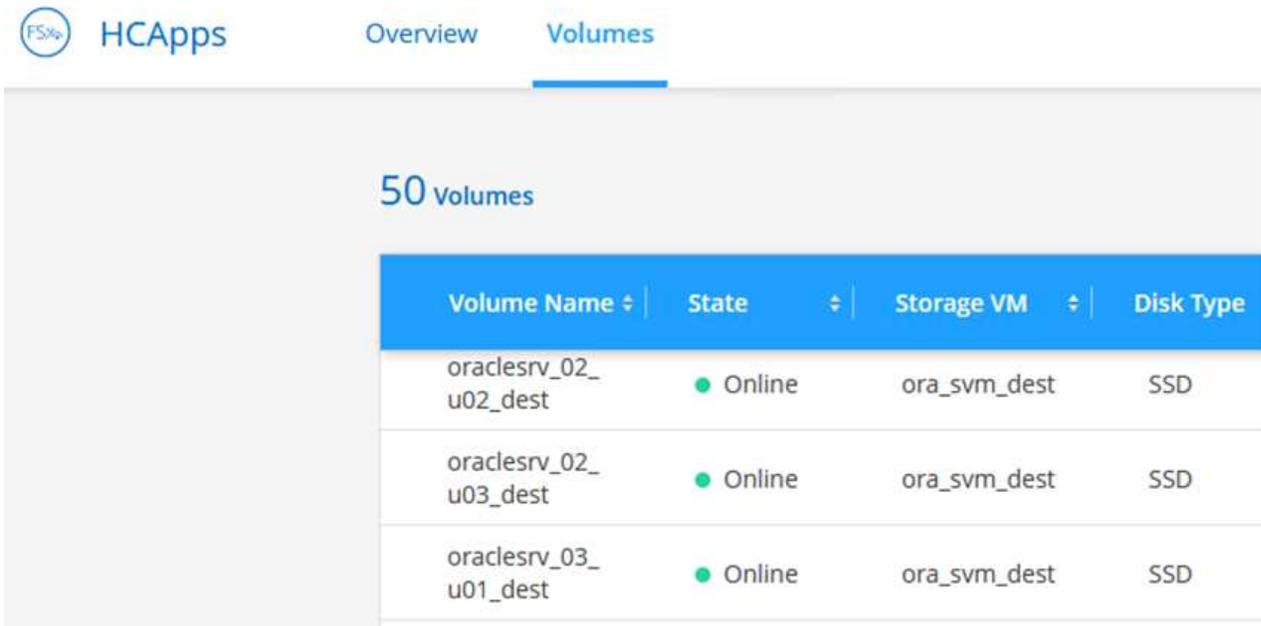
Cancel

Update

Oracle ServerにNFSボリュームをマウントする

Cloud Manager では、Oracle データベース ファイルとログを含む NFS ボリュームをマウントするための正しい NFS LIF IP アドレスを指定したマウント コマンドを取得できます。

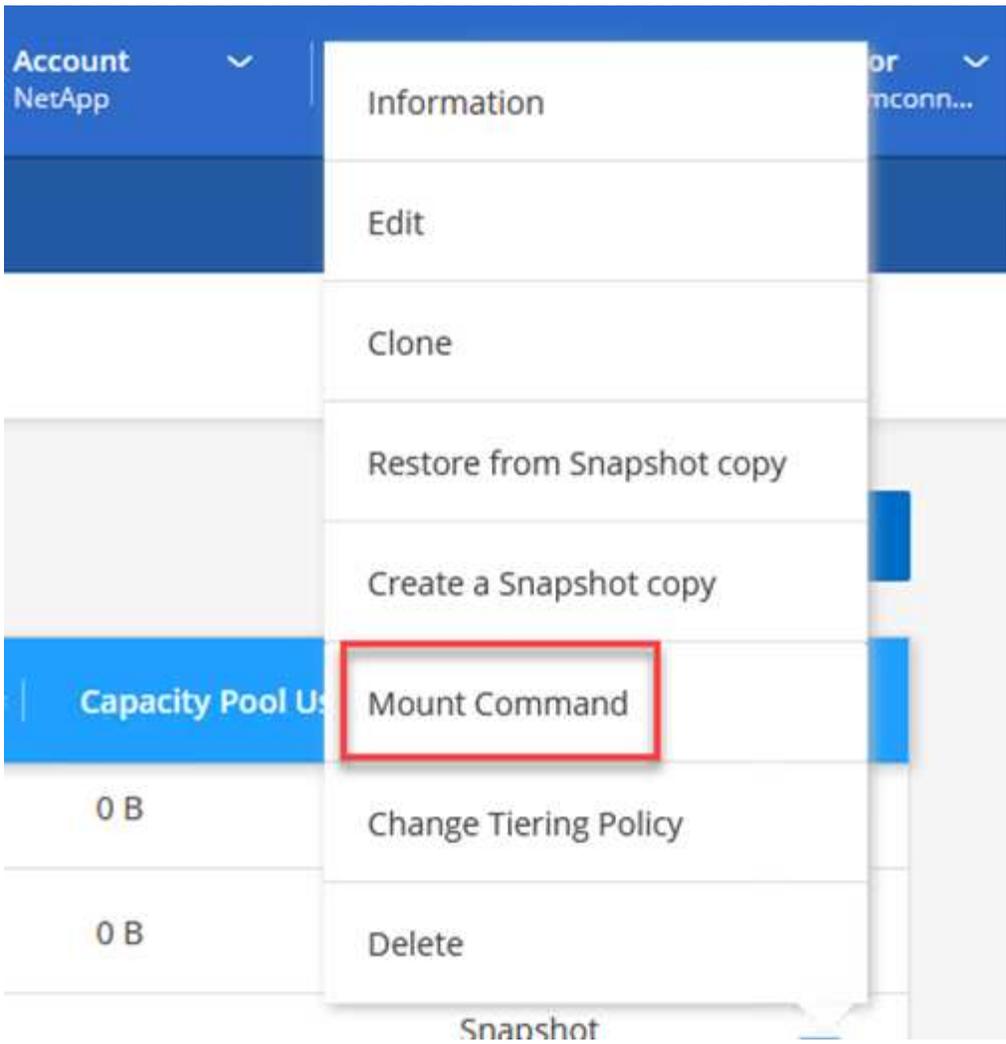
1. Cloud Manager で、FSx クラスターのボリュームのリストにアクセスします。



The screenshot shows the Cloud Manager interface for an FSx cluster. The 'Volumes' tab is selected, showing a list of 50 volumes. The table below displays the first three volumes:

Volume Name	State	Storage VM	Disk Type
oraclesrv_02_u02_dest	Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	Online	ora_svm_dest	SSD

2. アクション メニューから [マウント コマンド] を選択し、Oracle Linux サーバーで使用するマウント コマンドを表示およびコピーします。



Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```

 Copy

3. NFS ファイル システムを Oracle Linux Server にマウントします。NFS 共有をマウントするためのディレクトリは、Oracle Linux ホストにすでに存在します。
4. Oracle Linux サーバーから、mount コマンドを使用して NFS ボリュームをマウントします。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracle データベースに関連付けられているボリュームごとにこの手順を繰り返します。



再起動後もNFSマウントを永続化するには、`/etc/fstab`マウント コマンドを含めるファイル。

5. Oracle サーバーを再起動します。Oracle データベースは正常に起動し、使用可能になります。

フェイルバック

このソリューションで概説されているフェイルオーバー プロセスが正常に完了すると、SnapCenterとVeeam は AWS で実行されているバックアップ機能を再開し、FSx ONTAPは元のオンプレミス データセンターとの既存のSnapMirror関係がないプライマリ ストレージとして指定されます。オンプレミスで通常の機能が再開されたら、このドキュメントで説明されているプロセスと同じプロセスを使用して、オンプレミスのONTAPストレージ システムにデータをミラーリングできます。

このドキュメントでも説明されているように、SnapCenterを構成して、FSx ONTAPのアプリケーション データ ボリュームをオンプレミスのONTAPストレージ システムにミラーリングすることができます。同様に、スケールアウト バックアップ リポジトリを使用してバックアップ コピーを Amazon S3 に複製するようにVeeam を構成して、それらのバックアップがオンプレミス データセンターにある Veeam バックアップ サーバーにアクセスできるようにすることができます。

フェイルバックはこのドキュメントの範囲外ですが、フェイルバックはここで概説した詳細なプロセスとほとんど変わりません。

まとめ

このドキュメントで紹介するユースケースは、NetAppとVMware の統合を強調する実証済みの災害復旧テクノロジーに重点を置いています。NetApp ONTAPストレージ システムは、実績のあるデータ ミラーリング テクノロジーを提供し、組織がオンプレミスと主要なクラウド プロバイダーが提供するONTAPテクノロジーにまたがる災害復旧ソリューションを設計できるようにします。

FSx ONTAP on AWS は、SnapCenterおよびSyncMirrorとのシームレスな統合を可能にし、アプリケーション データをクラウドに複製するソリューションの 1 つです。Veeam Backup & Replication は、NetApp ONTAP ストレージ システムと適切に統合され、vSphere ネイティブ ストレージへのフェイルオーバーを提供できる、もう 1 つのよく知られたテクノロジーです。

このソリューションは、SQL Server および Oracle アプリケーション データをホストするONTAPシステムのゲスト接続ストレージを使用した災害復旧ソリューションを提示しました。SnapCenterとSnapMirrorは、ONTAPシステム上のアプリケーション ボリュームを保護し、クラウドにある FSx または CVO に複製するための、管理しやすいソリューションを提供します。SnapCenter は、すべてのアプリケーション データをVMware Cloud on AWS にフェイルオーバーするための DR 対応ソリューションです。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。